



PhD thesis

**Propaganda, surveillance and cyberspace: consequences of  
online dirty tricks**

**Ogbogu, D.**

---

Full bibliographic citation: Ogbogu, D. 2020. Propaganda, surveillance and cyberspace: consequences of online dirty tricks. PhD thesis Middlesex University

Year: 2020

Publisher: Middlesex University Research Repository

Available online: <https://repository.mdx.ac.uk/item/1894qx>

---

Middlesex University Research Repository makes the University's research available electronically.

Copyright and moral rights to this work are retained by the author and/or other copyright owners unless otherwise stated. The work is supplied on the understanding that any use for commercial gain is strictly forbidden. A copy may be downloaded for personal, non-commercial, research or study without prior permission and without charge.

Works, including theses and research projects, may not be reproduced in any format or medium, or extensive quotations taken from them, or their content changed in any way, without first obtaining permission in writing from the copyright holder(s). They may not be sold or exploited commercially in any format or medium without the prior written permission of the copyright holder(s).

Full bibliographic details must be given when referring to, or quoting from full items including the author's name, the title of the work, publication details where relevant

(place, publisher, date), pagination, and for theses or dissertations the awarding institution, the degree type awarded, and the date of the award.

If you believe that any material held in the repository infringes copyright law, please contact the Repository Team at Middlesex University via the following email address: [repository@mdx.ac.uk](mailto:repository@mdx.ac.uk)

The item will be removed from the repository while any claim is being investigated.

See also repository copyright: re-use policy: <https://libguides.mdx.ac.uk/repository>



# **Propaganda, Surveillance and Cyberspace: Consequences of Online Dirty Tricks.**

**David Emeka Nnamdi Ogbogu**

**A Thesis Submitted to Middlesex University for the Degree of  
Doctor of Philosophy in the School of Law**

**2020**

**Supervisors:**

**1st Supervisor: Dr Peter Hough,  
Middlesex University**

**2nd Supervisor: Dr Tine Monk  
Middlesex University**

---

## Abstract

---

In the 21<sup>st</sup> century, cyberspace has become an anarchic medium of defamatory, false information. Intelligence services are attempting to subvert and shape the perception of citizens around the world, in the absence of a sovereign liberal international arbiter that acts above all nations. Of late, intelligence services such as Britain's Government Communications Headquarters (GCHQ), America's Federal Bureau of Investigation (FBI), Russia's GRU service and non-state groups such as CyberBerkut have been caught disseminating erroneous information on the Internet. As a means of protecting democracy from hostile states and non-state groups, Western intelligence services have chosen to wield propaganda and surveillance measures.

Leaked documents have revealed GCHQ's propaganda aims of altering the outcome of online polls, setting up fake aliases to communicate with the world, and leaking confidential information to the press and blogs. The latter manoeuvre is ironically symmetrical with Russia's alleged ploy of warping perception in America's 2016 presidential election. Moreover, the FBI's fake terrorist propaganda website that was a part of a scheme to monitor and encourage US citizens to fight in Syria. Betwixt in the multitudes of fractured realities is the individual citizen, who is burdened with the task of deciphering truths, half-truths and outrageous lies from one another.

Amidst the confusion, are citizens capable of seeing through the schemes of nefarious actors online? Will society descend into what Walter Lippmann has described as a phantom public that is devoid of lucid thought and the confidence to endure the modern cyber terrain? This research sets out to explore the ramifications of modern propaganda and surveillance measures in society. Specifically, this research endeavours to appropriate the concept of Ontological (in) Security (OIS) in order to assess how states and citizens react to online dirty tricks campaigns. I argue that state attempts to manage a Realist information environment with dirty tricks can lead to creating additional issues that produce OIS both domestically and abroad.

---

## Acknowledgement

---

Although I do like to think of myself as a young genius, I could not have completed this PhD without the support of several people around me. First of all, I would like to thank God for helping me to overcome many obstacles in life. Secondly, I would like to thank both of my research supervisors who have stuck by me throughout this process. Dr Peter Hough took a gamble on me in 2016 and agreed to be my director of studies, even though my application was handed in very late! From the start to the end of this process, Dr Hough has helped to transform me from a raw Masters student to an accomplished PhD holder. Dr Tine provided an incredible amount of support and helped me take my thesis to a new level. For this, I am forever grateful. I would like to also thank my support officer 'Auntie' Patricia Babatunde for putting a support platform in place for me.

Moreover, I would like to take this opportunity to thank Laura Newman and Ruth Houghton from Middlesex University Library. Without their endless insight into referencing it would have taken me a million years to complete this thesis! Both Laura and Ruth sacrificed their time to answer a continuous stream of issues that I ran into and not once responded with resentment. They are outstanding and exemplary members of staff at Middlesex University library. Laura and Ruth, your contribution will always be remembered.

I would also like to thank both of my former managers at the Charity Commission. Nick Donaldson and Alex Gifford who employed me as a full-time intelligence researcher, while I was in my third year for my PhD. Throughout my time at the Commission, both Nick and Alex made life incredibly comfortable which enabled me to somehow do 80 hours a week between university and the Commission. Janet Mernane 'second mum' Soames Shillingford and Monica Davidson took great care of me at the Commission. Whenever I looked exhausted I was always looked after at the Commission. I am incredibly grateful to those who supported me through difficult times. Without the support of those close to me at the commissions undertaking over 80 hours of work per week would have been impossible.

Within my personal social network, my mother and sister Claire Ogbogu have been the most crucial components in my life and throughout this PhD process. Financially my sister and mother have supported me through difficult periods without hesitation. Additionally, my mum and sister have encouraged me throughout this process when I was close to giving up. I cannot stress how integral my mother and sister have been in my life. Thank you for your loyalty and support.

Furthermore, I would like to thank my friends who have played an integral role in helping me complete my PhD thesis. Without, Fela Latilo, Kwasi Adomakoh, Alex McDonald, Mazan Aref, Shervin Afshar Alam, Alaister Cuaresma, Daniel Ahmadi, and Shervin I would have definitely thrown the towel in and given up on my PhD. All of these brothers have taken so much time from their personal lives to keep me motivated with high spirits. I would also like to thank my 'Ghanian' friends Aaron Yamoha and Jerimiah Anson for continuously supporting me and always be available when I needed guidance and motivation. Mishax Foster, a humble and kind friend of mine has been encouraging me for years to persevere within academia. Without his consistent positivity, I would have continued to work in retail and abandoned my dreams. 'Never give up big man' has stuck with me for years, thank you Mishax.

In addition, I would like to thank Uthman Odutayo, for spending a considerable amount of time providing me with crucial life advice after I was released from Queens Park Rangers (QPR). During this turbulent up until contemporary times, Uthman has guided me and sacrificed a significant amount of time to make sure I was balancing University work with real-world experiences and most importantly a social life! Uthman has been a fundamental positive figure in my life. Without his long term friendship, my choices in life may have been significantly different! Lastly, although he has long passed, I owe my inspiration and determination to the late Malcolm X. At the age of 19, Malcolm X's speeches encouraged me to be a dignified emboldened young black man and to take research and education seriously. Additionally, I would like to thank Professor Noam Chomsky. Professor Chomsky's courage and wealth of knowledge has inspired me to be the best I can be within the field of International Relations and Propaganda.

**Research Repository Thesis Deposit Agreement**

[Redacted]

[Redacted]



[Redacted]

[Redacted]

[Redacted]



**Candidate Declaration form**

[Redacted]

[Redacted]

---

## Abbreviations Table

---

<b>Abbreviation</b>	<b>Full Name</b>
<b>AI</b>	Artificial Intelligence
<b>APT28</b>	Advanced Persistent Threat 28
<b>BW</b>	Biological Warfare
<b>CG5824-S</b>	*Code name for FBI SOLO informant
<b>CHS</b>	Confidential Human source
<b>CIA</b>	Central Intelligence Agency
<b>CNE</b>	Computer Network Exploration
<b>CNO</b>	Computer Network Operation
<b>COMPROP</b>	Computational Propaganda Research Project
<b>COINTELPRO</b>	Counter Intelligence Program
<b>CPA</b>	Communist Party Australia
<b>CPUSA</b>	Communist Party United States of America
<b>CID</b>	Criminal Investigation Department
<b>DCI</b>	Director of Central Intelligence
<b>DDOS</b>	Distributed Denial of Service attacks
<b>DOD</b>	Department of Defence (US)
<b>DGC</b>	Digital Geneva Convention
<b>DIA</b>	Defence Intelligence Agency (US)
<b>DNC</b>	Democratic National Committee
<b>DRIPA</b>	Data Retention Investigatory Powers Act 2014

<b>DTLINEN</b>	*US Code name for an East German propaganda campaign against communist elements
<b>ECJ</b>	European Court of Justice
<b>EI</b>	Equipment interference
<b>ELINT</b>	Electronic Intelligence
<b>EU</b>	European Union
<b>FAS</b>	Federation of American Scientist
<b>FBI</b>	Federal Bureau Investigation
<b>G7</b>	Group of Seven *worlds advanced industrialised economies
<b>GCHQ</b>	Government Communications headquarters
<b>GCSB</b>	Government Communications Security Bureau
<b>HMG</b>	Her Majesty's Government
<b>HIS</b>	Homeland Security Investigations
<b>HUMINT</b>	Human Intelligence
<b>ICC</b>	International Criminal Court
<b>ICE</b>	Immigration and Customs Enforcement
<b>ICJ</b>	International Court of Justice
<b>IGO</b>	Intergovernmental organisations
<b>IO</b>	Information Operations
<b>IPA</b>	Investigatory Powers Act 2016
<b>ISO</b>	International Organization of Standardisation
<b>IR</b>	International Relations
<b>IRD</b>	Information Research Department
<b>ISO</b>	International Organization of Standards
<b>JTRIG</b>	Joint Threat Research Intelligence Group

<b>JPOTF</b>	Joint Psychological Operations Task Force
<b>KKK</b>	Ku Klux Klan
<b>MCP</b>	Malayan Communist Party
<b>MI5</b>	*British domestic security intelligence service
<b>MI6</b>	* British international security intelligence service
<b>MLK</b>	Martin Luther King
<b>NGO</b>	Non-Governmental Organisations
<b>NKPA</b>	North Korean People's Army
<b>NSA</b>	National Security Agency
<b>NSC</b>	National Security Council (US)
<b>NTNI</b>	Net Talon National Initiative
<b>OCE</b>	Online Covert Employee
<b>ODNI</b>	Office of the Director of National Intelligence
<b>OECD</b>	Organisation for Economic Cooperation and Development
<b>OHCHR</b>	Office of the United Nations High Commission for Human Rights
<b>OIS</b>	Ontological In Security
<b>OPCW</b>	Organisation for the Prohibition of Chemical Weapons
<b>OS</b>	Ontological Security
<b>OSS</b>	Office of Strategic Services (US)
<b>TEI</b>	Targeted Equipment Interference
<b>PR</b>	Public Relations
<b>PSYOP</b>	Psychological Operations
<b>RAM</b>	Revolutionary Action Movement



<b>SDECE</b>	Service de documentation extérieure et de contre-espionnage (External Documentation and Counter-espionage Service: English Translation)
<b>SOLO</b>	*SOLO was the codename for an FBI covert Counter Intelligence operation against the CPUSA the Soviet Union and Communist China.
<b>SIGINT</b>	Signals Intelligence
<b>SWF</b>	Sovereign Wealth Fund
<b>UCE</b>	Under Cover Employee
<b>UK</b>	United Kingdom
<b>UN</b>	United Nations
<b>UNAMA</b>	United Nations Assistance Mission In Afghanistan
<b>US</b>	Unites States
<b>USA</b>	Unites States of America
<b>USAID</b>	United States Agency for International Development
<b>USAF</b>	United States Air Force
<b>USG</b>	Unites States Government
<b>USIC</b>	United States Intelligence Committee
<b>VCD</b>	Video Compact Disk
<b>VEP</b>	Vulnerabilities Equities Policy (US)
<b>WW1</b>	World War 1
<b>WW2</b>	World War 2

---

## Contents

---

Abstract .....	2
Acknowledgement.....	3
<b>Student details .....</b>	<b>Error! Bookmark not defined.</b>
<b>Candidate Declaration .....</b>	<b>Error! Bookmark not defined.</b>
<b>2 Material submitted for another award.....</b>	<b>Error! Bookmark not defined.</b>
<b>3 Research Ethics .....</b>	<b>Error! Bookmark not defined.</b>
<b>Statement by the Student.....</b>	<b>Error! Bookmark not defined.</b>
Abbreviations Table .....	12
Chapter 1: Introduction .....	19
1.1 Aims and Objectives .....	28
1.2 Why Focus on Intelligence Services of Western States?.....	30
1.3 Academic Gap in Knowledge.....	37
1.4 What are the far-reaching Implications of Propaganda and Surveillance?.....	39
1.5 Propaganda and its Gravity .....	43
1.6 The State and Private Companies participation in Propaganda and Surveillance .....	51
1.7 Propaganda and Surveillance: Two Sides of the Same Coin.....	63
1.8 Walter Lippmann and the Phantom Public.....	66
1.9 In What Ways is the Modern Public Irrational and Susceptible to Propaganda? .....	76
1.10 State Crime, Human Rights and the Divided Self .....	81
1.11 The Self and its Divisions .....	87
1.12 State Crime.....	91
1.13 Human Rights Defined.....	99
1.14 State Crimes and the Divided Self.....	103
1.15 International Relations Theory and Cyberspace.....	112
1.16 Intelligence Services and the Defence of Empire and Spheres of Influence. ....	118
1.17 Methodology .....	128
1.18 Structure of the Thesis.....	136
Chapter 2: Definitions and Context.....	139
2.1 An overview of Realism and Anarchy .....	146
2.2 Anarchy .....	151
2.3 Neo-Realism.....	153
2.4 Liberalism.....	155
2.5 Liberal Cosmopolitanism and the Digital Geneva Convention.....	158
2.6 Cooperation .....	161
2.7 Cyberspace .....	165
2.8 Intelligence .....	167
2.9 Cybersecurity .....	168
2.10 Cyber Espionage and Cyber-Attacks.....	169
2.11 Surveillance and Mass Surveillance .....	172
2.12 Propaganda .....	179
2.13 The Sham Universe and the Democratic Proselytisation of Terrorism .....	182
2.14 Risk .....	185
2.15 Ontological (In) Security.....	185
2.16 Tainted Leaks .....	187
Chapter 3: History and Context of Propaganda and Surveillance 20 <sup>th</sup> Century Surveillance.....	188
3.1 The WW1 .....	188
3.2 The WW2 .....	190
3.3 The Cold War and the Vagaries of Intelligence Collection.....	192
3.4 Photoreconnaissance and America’s Perceived Military Gap With the Soviet Union .....	195
3.5 IGLOO WHITE and ELINT During the Vietnam War.....	198
3.6 OPERATION SOLO and The FBI’s HUMINT Mole.....	199
3.7 COINTELPRO, Black Extremism and the FBI’s Domestic Psychological Warfare .....	200
3.8 The 21 <sup>ST</sup> Century.....	204
3.9 The Evolution of Propaganda from the 20 <sup>th</sup> to the 21 <sup>st</sup> Century .....	210

3.10	OSS Propaganda during WW2: Eugenics and Overt Propaganda in Nazi Germany, America and Britain.....	214
3.11	Cold War Propaganda .....	227
3.12	The IRD anti-Communist propaganda: From Nigeria to Latin America.....	231
3.13	The IRD in Latin America.....	233
3.14	The CIA in Latin America.....	235
3.15	COINTELPRO, Black Nationalists and the FBI's Propaganda.....	238
3.16	Cyber Propaganda in the 21 <sup>st</sup> Century.....	241
3.17	Digital Geneva Convention: Anarchy and State/Non-State Surveillance Ambitions in Cyberspace.....	241
3.18	The Digital Geneva Convention.....	244
3.19	Subverting Non-State Efforts .....	251
Chapter 4:	Literature Review .....	253
4.1	The Surveillance Literature Review .....	253
4.2	Post Snowden .....	257
4.3	Privacy and surveillance.....	260
4.4	Ontological Security.....	261
4.5	Hactivism .....	264
4.6	Democracy and Intelligence .....	265
4.7	Ethics of Intelligence and the Democratic State.....	269
4.8	International Norms, Ethics and Intelligence .....	275
4.9	Media and Intelligence .....	277
4.10	Privacy and Intelligence .....	278
4.11	Democracy and Propaganda.....	280
4.12	Media as Propaganda Platforms for the State.....	287
4.13	Control.....	288
4.14	Robot Trolling and Modern Methods of Propaganda.....	290
Chapter 5,	Case Study 1: Propaganda, Surveillance and Ontological (In) Security a Case of West vs the East .....	292
5.1	JTRIG, Russia and the US 2016 Presidential Elections.....	294
5.2	Senator Eric Swalwell .....	297
5.3	Senator Mark Warner.....	299
5.4	Senator Elizabeth Warren .....	303
5.5	Conclusion .....	309
Chapter 6,	Case Study 2: The Democratic Proselytisation of Non-State Terror and the FBI's Sham Universe .....	311
6.1	Net Talon National Initiative.....	313
6.2	The OCE's and Entrapment.....	315
6.3	Abdella Tounisi .....	319
6.4	Analysis.....	334
6.5	Conclusion.....	341
Chapter 7	Case Study 3: Tainted Leaks, Forgeries, and Propaganda. A Case of David Satter and the French Elections.....	343
7.1	Phantom Public .....	344
7.2	A Recap of the Soviet Union and CIA Backed KgU Forgeries.....	345
7.3	Tainted Leaks .....	349
7.4	Analysis.....	353
7.5	Conclusion.....	363
Chapter 8	Case Study 4: Staged Psychological Warfare and Constructed Realities .....	365
8.1	North Korea Psychological Warfare.....	367
8.2	The Pentagon, Bell Pottinger and Staged Psychological Warfare in Iraq .....	369
8.3	Conclusion.....	377
Chapter 9	Thesis Conclusion.....	378
9.1	Contribution to Knowledge .....	382
9.2	Cross Case Study Reflections.....	384
9.3	Chapter 5 .....	384
9.4	Chapter 6 .....	385

9.5	Chapter 7 .....	387
9.6	Chapter 8 .....	388
9.7	Limitations of the Study .....	389
9.8	Final Remarks .....	389
	Reference List .....	392
	Appendices .....	497
	Appendix 1 Snapshot of Information That Explains the Nature of the IRD.....	498
	Appendix 2: Snapshot of IRD Delivery of Books to Nigeria.....	499
	506Appendix 3: Snapshot of IRD Contacts in Northern Nigeria.....	500
	507Appendix 4: Snapshot of IRD Contacts in Northern Nigeria.....	501
	Appendix 5: Snapshot of IRD Contacts in Northern Nigeria.....	502
	Appendix 6: Snapshot of IRD Contacts in Northern Nigeria.....	503
	Appendix 7: Snapshot of IRD Reflection Concerning Nigeria’s Stability and Prospects.....	504
	Appendix 8: Snapshot of Foreign Office (IRD) Concerns about Threats of Subversion in Nigeria	505
	Appendix 9: Snapshot of IRD Material in Nigeria’s Press.....	512
	Appendix 10: Snapshot of the UK Foreign Office Policy in Latin America.....	507
	Appendix 11: Snapshot of IRD Material Distribution in Colombia.....	508
	Appendix12: Snapshot of Foreign Office Information Policy towards Fidel.....	509
	Appendix 13: Snapshot of IRD Material in Latin America.....	510
	Appendix 14: Snapshot of IRD Material in Latin America’s Media.....	511

---

## Chapter 1: Introduction

---

Cyberspace is at risk of being inexorably bound to the constant threat of propaganda and surveillance campaigns that attempt to fracture and subvert reality as a means of shaping perception. Intelligence services from global powers such as Russia, China, Britain and America have made concerted efforts to warp the perception of citizens all over the world by unleashing deceitful propaganda online under the guise of false identities. Often citizens are unaware that they are being deceived by bot trolls or online human covert operatives. Moreover, in light of media-based leaks from investigative journalists and Edward Snowden, it has become clear that Britain's Government Communication Headquarters (GCHQ) the Federal Bureau of Investigation (FBI), Russia's Military intelligence the GRU and Chinese state operatives have engaged in propaganda and surveillance campaigns in which intelligence sharpens domestic and global influence endeavours.

As a consequence of covert intelligence operations becoming public knowledge, faith in democratic institutions is at risk of being engulfed by cynicism, conspiracy theories and OIS (Giddens, 1990, p. 92; Giddens, 1990, p. 94). Surveillance can be defined 'as all sorts of monitoring from the most rudimentary type of visual observation and recording of information, to genetic testing, electronic monitoring and the use of statistical analysis in the construction of categories and prediction of [behaviour]' (Zureik, 2003, p.37). Whereas propaganda can be defined as the 'dissemination of ideas intended to convince people to think and act in a particular way and for a particular persuasive purpose' (Welch, 2013; p.2).

The seductive and coercive grip of propaganda has helped to exacerbate atrocities witnessed in Nazi Germany, radicalise young people to fight for DAESH in Syria and convince many world leaders and citizens that Saddam Hussein had chemical weapons. Throughout the 20<sup>th</sup>-century intelligence services made use of propaganda and surveillance to shape the perception of domestic groups and the citizens of foreign

adversaries. The FBI regularly monitored the Black Panthers during the Bureau's COINTELPRO information war on *Black Extremism* which often led to the Black Panthers being unjustly smeared by propaganda (FBI, 1967, p.7; FBI, 1969, p.8). Similarly, America's Central Intelligence Agency (CIA) capitalised on intelligence ascertained from its contacts in Europe on Nikita Khrushchev inflammatory critique of Joseph Stalin. The Khrushchev speech was later used to highlight division within the Soviet Union and influence ideological fracture points (Melman, 2007; Ranelagh, 1987, p. 287).

For the sake of clarity, intelligence can be defined as 'information, not always available in the public domain, relating to the strength, resources, capabilities and intentions of a foreign country that can affect our lives and the safety of our people' (Walters, 1978, p.621, cited in Warner, 2008). Essentially intelligence is information-based knowledge that is derived from covert or overt inquiries, monitoring and the interception of signals which help to inform governments and subsidiary organs of the state or non-state groups about the intentions of a domestic and foreign target. Intelligence can be obtained by online and offline sources and methods.

However, in contemporary times intelligence services have capitalised on the expansive domain and interconnectivity of cyberspace, by using intrusive and relentless surveillance tactics in conjunction with potent propagandised messages. In effect, both propaganda and surveillance can be described as necessary tools to protect a nation from the hostile activity of foreign adversaries and domestic criminals. In the 21<sup>st</sup>-century intelligence services of multiple nations have launched propaganda and surveillance campaigns to warp the perception of citizens throughout the world.

Fake terrorist websites created by FBI, fake propaganda aliases created by Britain's intelligence services GCHQ and misleading information secreted by hacktivists are just a few examples of how states and non-state groups are willing to undermine democratic values to warp perception online. In the past propaganda would have manifested as physical leaflets, radio communication, and public polemicists that launched verbal attacks at or towards their targets. Of late, propaganda is comprised of autonomous or human-controlled bots and trolls that inject propaganda into platforms such as Facebook, Twitter, Instagram, YouTube and other platforms. Moreover, the advancement of

technology has enabled Deep Fakes to replicate the digital likeness of a target in order to misattribute opinions of someone else to the target and make it appear as if the target of disinformation has said something outlandish (Dack, 2019). Such insidious information measures are not exclusively used by authoritarian regimes. In contrast, the intelligence services of Western states such as Britain and America have used false personas online to shape information (Fishman and Greenwald, 2015; Klass, 2016, p.49; ‘United States Of America v. Abdella Ahmad Tounisi, 2013, p.19).

Of late, the United States Intelligence Community (USIC) has concluded that state and non-state actors ‘remain undeterred from conducting reconnaissance, espionage, influence, and even attacks in cyberspace’ (ODNI, 2017[a], p.5). Moreover, in the assessment of MI5 ‘[a] wide range of hostile actors use cyber to target the UK. They include foreign states, criminals, "hacktivist" groups and terrorists...Hostile actors conducting cyber espionage can target the government, military, business and individuals’ (MI5, n.d.[a]). GCHQ has informed the UK intelligence and security committee that ‘International law applies to state acts in cyberspace’ even though this assertion is not underpinned by any binding international agreements (Parliament. House of Commons, 2017, p.51). Currently, the United Nations (UN) General Assembly has adopted two proposals to establish rules or norms concerning responsible behaviour in cyberspace for the greater good of every nation (UN, 2018[a]).

However, so far the UN has failed at restraining nations and non-state actors from engaging in aggressive propaganda and surveillance campaigns. In the absence of a coercive unilateral legal and moral arbiter that acts above every nation, states have chosen to operate in cyberspace to disrupt information systems, steal information and warp perception to meet domestic and foreign policy objectives. Consequently, nations within the international arena have adopted ‘Realist’ principles that revolve around confrontation and aggressive competition with other states and applied them to cyberspace to remedy the lack of international protection against information operations (Havercroft and Prichard, 2017, p.258; Karatzogianni and Robinson, 2017, p.283; Craig and Valeriano, 2018, p.85). This move has brought the UN’s concept of ‘Cyber Stability’ into great scrutiny Rudnik, Miller and Levy, 2015, p.13). Cyber stability is defined as ‘[a] geostrategic condition whereby users of the cyber domain enjoy the greatest possible

benefits to political, civic, social, and economic life while preventing and managing conduct that may undermine those benefits at the national, regional, and international levels' (Rudnik, Miller and Levy, 2015, p.13). As such, cyberspace has been polluted by intelligence services with covert propaganda and left insecure as a result of advanced intrusive surveillance capabilities that are developing throughout the world.

Despite the defensive measures taken by states to protect their networks from hostile actors, nations have a vested interest in the fragile systems of other states. Nations such as China are 'believed to have more than 100,000 cyberwarfare hackers and highly trained personnel to focus more on warfare using integrated networks and satellites' (Kremling and Parker, 2018, p.114-115). In 2018, the US Department of Defense (DOD) pledged that it would 'conduct cyberspace operations to collect intelligence and prepare military cyber capabilities to be used in the event of crisis or conflict' (Department of Defense (US), 2018, p.3). Additionally, GCHQ and the National Security Agency (NSA) are at the helm of the Anglosphere Five Eyes intelligence alliance that peruses a policy of undermining the integrity of networks of both enemy and friendly states on a global scale (Gallagher and Hager, 2015). Similarly, British Bulk Equipment Interference (EI) and Targeted Equipment Interference (TEI) permit intrusive cyber-surveillance and penetration of electronic devices around the world (House of Commons, 2015[a], p.1; House of Commons, 2015[b], p.1).

Despite international sanctions, North Korea has assembled a formidable cyber force that was responsible for hacking Sony (FBI, 2014). Furthermore, the resurgence of Russia has been correlated with alleged cyber propaganda and surveillance campaigns throughout Europe and infamously against the US during the (US) 2016 presidential elections (NCSC, 2018[a]; ODNI, 2017[b], p.6). Overall, within this new cyber boiling pot, '[m]any governments have been strengthening their cyber warfare capabilities for both defensive and offensive purposes' (Forelle et al., 2015, p.1).

Non-state entities such as WikiLeaks and Anonymous, have also played their role in exposing government surveillance and revealing the identity of Ku Klux Klan (KKK) members by hacking the Klan and exposing their social media accounts (WikiLeaks, 2017a; WikiLeaks, 2017b; AnonHQ, 2014). However, beyond surveillance 'the rise of cyberspace has transformed both the meaning and opportunity for propaganda' (Baines



and O'Shaughnessy, 2014, p.9). The UK governments 2011 Cybersecurity Strategy rightly pointed out that '[c]yberspace is already used by terrorists to spread propaganda, radicalise potential supporters, raise funds, communicate and plan' (Cabinet Office (UK), 2011, p.14). On the contrary, in light of the Snowden affair and Glen Greenwald's coverage of the leaks, it is now clear that GCHQ is using dirty tricks in cyberspace to warp perception online. Dirty Tricks can be described as 'underhanded stratagems for obtaining secret information about or sabotaging an enemy or for discrediting an opponent (as in politics)' (Meriam-Webster, 2019).

For example, GCHQ tasked its subunit Joint Threat Research Intelligence Group (JTRIG) with carrying out propaganda campaigns around the globe. In particular, Operation Quito was a JTRIG propaganda and surveillance campaign that used 'offensive cyber operations to prevent Argentina from taking the islands' (Fishman and Greenwald, 2015). Of late Iran, much like its democratic counterpart (UK) has chosen to engage in online dirty tricks in the form of creating and pretending to be genuine US and British news outlets (FireEye, 2018, p.3). During the Cold War the US State Department and Britain's covert Information Research Department (IRD) injected anti-Sukarno propaganda into Indonesia in order to instigate Sukarno's removal from the presidential office (Easter, 2005, p.58; Office of the Historian, 1965).

After the 'abortive coup' attempt by the 30 September Movement and alleged elements of the ruling PKI Communist Party, Indonesia spiralled into a bloody civil war (Easter, 2005, p.56). Fast forward to the modern cyber era, Russia is alleged to have interfered in America's 2016 presidential election in a far more sophisticated methodology than covert radio propaganda (ODNI, 2017[b], p.6). NATO has also been concerned about Russia's Hybrid Trolls that have allegedly attempted to disrupt public opinion in Latvia (Spruds et al., 2016, p.10). Similarly, China's 50-cent commentators also known as the fifty-cent army, Mexico's Penabots and Venezuelan bots have surfaced as modern online attempts by nations to influence public opinion (Forelle et al., 2015, p.1; Han, 2015, p.105; King, Pan and Roberts, 2013, p.484; Porup, 2015; Sullivan, 2014, p.32).

In light of the cyber information age, Pandora's Box is wide open. Intelligence services and their political masters mean to keep it this way, in order to shape cyberspace in the likeness of national security and foreign policy objectives. Looking back at the omen-like

words of Walter Davison it seems logical to assume that ‘[t]he pervasiveness of international propaganda has increased not only as a result of the availability of new channels but also because of the recognition of propaganda as a regular, permanent function of national governments, in peace as well as in war’ (1971, p.5).

At a glance, cyberspace is permeated with a litany of actors who are using propaganda and surveillance measures to sway the perception of domestic and foreign citizens. The primary catalyst that prompted this thesis is the fact that ‘Intelligence agencies have learned to use social media to their advantage. By using fake identities, they can create an illusion of support for ideas’ (Hochwald, 2013, p.31). Fake identities, or at least the option to mask one's character is not necessarily novel. In spite of this, fake identities have wreaked havoc in cyberspace due to the multitude of personas that can be created by one person or an intelligence service against a target. Thanks to the Snowden leaks concerning GCHQ’s subunit, JTRIG, Snowden has revealed a new playbook of online dirty tricks to influence the perception of foreign nations. According to the Snowden documents ‘[a] ll of JTRIG’s operations are conducted using cyber technology’ which specifically include:

*Uploading YouTube videos containing “persuasive” communications (to discredit, promote distrust, dissuade, deter, delay or disrupt)...Setting up Facebook groups, forums, blogs and Twitter accounts that encourage and monitor discussion on a topic (to discredit, promote distrust, dissuade, deter, delay or disrupt)...Establishing online aliases/personalities who support the communications or messages in YouTube videos, Facebook groups, forums, blogs etc...Establishing online aliases/personalities who support other aliases...Sending spoof e-mails and text messages from a fake person or mimicking a real person (to discredit, promote distrust, dissuade, deceive, deter, delay or disrupt)...Providing spoof online resources such as magazines and books that provide inaccurate information (to disrupt, delay, deceive, discredit, promote distrust, dissuade, deter or denigrate/degrade) (Dhami, 2011, cited in The Intercept, 2015[a], p.9).*

While concrete evidence is scant; an additional Snowden document revealed that ‘[t]wo of the Global team's current aims are regime change in Zimbabwe by discrediting the present regime, and preventing Argentina from taking over the Falkland Islands by conducting online HUMINT’ (Dhami, 2011, cited in *The Intercept*, 2015[a], p.8). The endeavour of discrediting the Zimbabwean regime and influencing opinion on the Falklands in Argentina was active as far back as 2011. JTRIG’s playbook of dirty tricks and Western efforts in general is an area that needs further attention in academia in conjunction with the concept of Ontological Security (OS) and OIS (Giddens, 1990, p. 92; Giddens, 1990, p. 94). In order to develop an understanding of propaganda and surveillance measures, it is necessary to explore how both tools can impact the ontological sense of security at the state and citizen level.

Cognisant of the fact that intelligence services around the world are attempting to warp perception online, it is fundamental that scholarly attention within the field of International Relations (IR) Sociology and Communication Studies and other relatable fields are drawn to this contemporary phenomenon. Currently, research is predominantly geared towards Russian cyber propaganda against Western and European nations (Giles, 2016, p.3; Jones, 2018; Lucas and Pomeranzev, 2016, p.10; Spruds *et al.*, 2016, p.10; Hulcoop *et al.*, 2017; ODNI, 2017[b], p.6). Although academics such as Bakir have covered Western efforts, a more considerable amount of scrutiny is required to help build an understanding of why states engage in covert propaganda (2015[a], p.133). Furthermore, there is a need to understand how the OS of citizens and nations are impacted by covert propaganda and surveillance campaigns.

Additionally, Western efforts to shape perception online with covert propaganda is an under-researched area within academia. It is unlikely that states and citizens will not be affected by the torrent of false information presented online as legitimate truths. As such, it is integral to establish some form of understanding concerning OS and the use of propaganda and surveillance to shape perception online. While the sociological concept of OS (Giddens, 1990, p.92; Giddens, 1991, p.36) has not entirely assimilated into the vernacular of IR scholars; there is a gap in knowledge concerning the ramifications of JTRIG’s playbook and the OIS of the nation-state. This thesis attempts to analyse the inevitable sense of OIS that states and citizens feel when cyber propaganda and

surveillance campaigns are revealed. Multiple theories can be used to interpret the current state of cyberspace, such as Liberalism and Marxism.

Nonetheless, Cyberspace is arguably inexorably bound to the Realist school of thought, in the sense that Realist tenets such as anarchy and self-help are a permanent feature of cyberspace. This claim does not vanquish elements of peaceful collaboration that takes place in cyberspace, nor does it undermine the crucial work that non-state groups such as FireEye Kaspersky, Sophos and other cybersecurity vendors that contribute to network security. However, the potency and pervasiveness of state and non-state propaganda and surveillance measures that have wreaked havoc in cyberspace without the UN being able to exercise decisive control of the situation, has left this domain associated and indeed imbued with realist tenets such as anarchy and self-help.

This ominous reality will exponentially increase the sense of fear and anxiety that pushes states to adopt defensive and offensive information-based measures to sway perception online. Due to the inability of (some) citizens to distinguish between *good* cyber propaganda and *bad* cyber propaganda, states are operating at increased thresholds to counter the nefarious *other* with similar dirty tricks to protect their respective national OS. Upon realisation that so many forces are at work to disrupt the truth for political gains, it begs the question as to how a citizen can survive this terrain without losing hope in his or her belief to be able to perceive information independently and discern the truth from fiction. Walter Lippmann's book *The Phantom Public* drastically undermined the public's capacity to understand and direct public affairs. Lippmann referred to citizens as a 'phantom' which is unable to grasp the deluge of information that would need to be digested daily to understand politics (Lippmann, 1993, p.67). From Lippmann's perspective:

*The private citizen today has come to feel rather like a deaf spectator in the back row, who ought to keep his mind on the mystery off there, but cannot quite manage to keep awake. He knows he is somehow affected by what is going on. Rules and regulations... taxes...and wars occasionally remind him that he is being swept along by great drifts of circumstances (Lippmann, 1993, p.3).*

Post-Snowden, the litany of dirty tricks, used by intelligence services and non-state groups in cyberspace, has encouraged me to investigate as to whether or not Lippmann's cynical assessment of society's capacity is relevant in contemporary times. Since the Snowden's leaks which revealed GCHQ's international propaganda ambitions dating back to 2011, nations such as Iran and Russia, two targets of GCHQ's propaganda, have increased the threshold of offensive cyber information campaigns (MacFarquhar, 2016; McClintok, 2017; FireEye, 2018, p.3) (see chapter 5). Iran has engaged in setting up fake American and British news sites to influence perception abroad (FireEye, 2018, p.3). In addition, Russia has engaged in cyber information warfare tactics of disseminating false information online through bots and trolls (ODNI, 2017[b], p.2). Indeed, it is true that the Russian information campaign on Facebook began between June of 2015 to May of 2017 in order to inflame social division during the Democratic National Committee (DNC) leaks, however GCHQ's online playbook was leaked in 2014 (Facebook, 2017; Greenwald, 2014[a]).

However, over a year before this Russian endeavour on Facebook commenced, in 2014 a leaked GCHQ document has revealed that British online operatives aimed to focus on propaganda, deception, mass messaging, pushing stories and alias development in cyberspace (EFF, 2014[a], p.4). A testament to GCHQ's willingness to poison the well of cyberspace, JTRIG's tactics included setting up honey traps, writing a blog purporting to be a victim of JTRIG's target as well as sending emails and texts to colleagues, neighbours and friends of targets (Greenwald, 2014[a]). Conscious of the fact that JTRIG's remit is international, British propaganda endeavours to warp perception abroad in order to alleviate its sense of OS has demonstrated to other nations that warping perception against multiple state adversaries is a serious online endeavour.

This political signal has encouraged other countries to use similar tactics to target the West in cyberspace (see chapter 5). Attempts by one state to fortify its sense of OS has encouraged other nations to emulate propaganda and surveillance campaigns which in the case of Russia, proved to be detrimental for the US. <sup>1</sup> Nonetheless, the concept of OS

---

<sup>1</sup> It is important to note that in 2015 researchers from the Citizens Lab discovered a disinformation campaign in Latin America that was believed to be conducted by a nation albeit unknown who this particular nation was. See <https://citizenlab.ca/2015/12/packrat-report/>

must be used to assess how states react to modern forms of propaganda campaigns which to date is seldom replicated as a form of academic inquiry.

---

## 1.1 Aims and Objectives

---

Little is known about GCHQ's activities, let alone the impact that their playbook or modern propaganda methods can have on society and rival nations. This research endeavours to address the gap in knowledge concerning JTRIG's playbook of dirty tricks that comprise of propaganda and surveillance tactics. Specifically, the first research aim is to demonstrate that attempts by states to mitigate OIS, can have a counterproductive effect in a Realist environment that pushes competitive countries into engaging in high-risk cyber intelligence operations, which in turn increases OIS. In other words, OIS among states is amplified by their clandestine intelligence activities that end up being replicated by other states once such measures become public knowledge.

Alternatively, as suggested by Ulrich Beck '[m]odern society has become a risk society in the sense that it is increasingly occupied with debating, preventing and managing risks that it itself has produced' (2006, p.332).<sup>2</sup> In a similar sense, nations can become imbued by a sense of risk and OIS that they have created for themselves by engaging in high-risk intelligence operations that backfire and reach public awareness (see chapter 6 and 8). In chapter 6 and 8, the United States Government (USG) attempted to curtail the level of OIS it faced by engaging in propaganda and surveillance methods to sway the perception of potential and actual terrorist sympathisers.

Chapter 8, in particular, focuses on covert propaganda becoming unearthed and revealed to the public, which makes claims against one or multiple states of creating staged psychological warfare more believable. The Pentagon worked with British Public Relations (PR) firm Bell Pottinger to edit videos using Al-Qaeda footage to discredit Al-Qaeda during the Second Gulf War. Subsequently, USG propaganda was produced and

---

<sup>2</sup> Some authoritarian regimes may not care as much about how they are perceived on certain issues. For example China has placed large portions of its Uighur minority Muslim population camps for re-education to help integrate Muslims into China. See <https://www.amnesty.org/en/latest/news/2018/09/china-up-to-one-million-detained/> China has denied that they have been forcibly placed in camps and continued to with its process of education to deal with its domestic issues with integration.

presented in Iraqi media as local news (The Bureau of Investigative Journalism, 2017). Moreover, the USG purposefully dropped propaganda in the form of CD's which contained Bell Pottinger's work in the homes of suspected terrorists in order to track where the propaganda would spread (The Bureau of Investigative Journalism, 2017). As a consequence of dealing with probabilities, the USG ended up crystallising terrorist ideation of individuals that may have decided to turn away from terrorism. Post-revelation of the USG's online operations makes it difficult to associate the truth with American narratives on international issues, much to the delight of America's adversaries that push anti-US propaganda. In other words, recent attempts by the USG to shape the information environment to better its OS often end up increasing what it fears, which is a lack of credibility in influencing foreign and domestic opinion.

Moreover, a second aim is to assess the impact that surreptitious propaganda and surveillance measures can have on public opinion. This aim is based on the modern information environment that is being shaped by a culmination of cyber-attacks and information campaigns. According to the Ministry of Defence (UK):

*The Russian invasion of Georgia was preceded by an intensive series of cyber attacks attempting to disrupt Georgian governmental and civilian online infrastructure. This inhibited the Georgian Government's ability to communicate their strategic narrative and enabled the Russians to claim there was popular support (as evidenced by the hackers who, it was said, were just ordinary Russians) for the invasion. The confusion generated by claim and counter-claim made it difficult for international opinion to bear weight. Russian cyber information superiority was an important factor in an integrated campaign (Ministry of Defence (UK), 2013, p.33).*

When considering the above assessment, can mistrust of information produce OIS that curtails the willingness of citizens to hold strong opinions? In the case of modern digital propaganda, once people become aware that *evidence* is nothing more than a secretly crafted ruse, OIS may cause people to be reluctant to engage or debate contentious topics due to the inability to verify the truth (see chapter 7). Furthermore, a sub-objective is centred on the work of Lippmann to assess whether or not the public is prepared to deal

with contemporary propaganda methods in the form of ‘tainted leaks’ (Hulcoop et al., 2017). Lippmann is critical of the public’s capacity to understand the fast pace of current affairs. However, is Lippmann’s negative approach congruent with today’s public? Is it permissible to refer to the public as a phantom public that is ill-equipped to deal with sophisticated or rudimentary cyber propaganda manoeuvres postulated by intelligence services and non-state groups? The above question concerning the phantom public will be addressed in Chapter 7.

It is important to note that this research endeavours to fill the gap in knowledge predominantly about Western intelligence services such as GCHQ and the FBI. Although, it is vital to note that other nations such as China have used online commentators to warp perception (Creemers, 2017, p.88-92). Additionally, while the concept of risk is sparingly employed, this research does not intend to go into detail or scholarship concerning the theoretical underpinnings of risk. Lastly, while it is essential for future researchers to quantify aspects of this research, I have chosen not to carry out structured or semi-structured interviews.

Undoubtedly, both the former and the latter are integral to academia. However, this specific research is geared towards my analysis of events that have already transpired while simultaneously extrapolating future risks that can occur as a result of current trends and incidents. I feel that it is imperative to help build the foundations of inquiry for the field of propaganda, surveillance and OS predominantly through document analysis. Perhaps in the future other researchers can build on the foundations I have laid.

---

## **1.2 Why Focus on Intelligence Services of Western States?**

---

In recent years a significant amount of research and media attention has been directed towards the propaganda and surveillance activities of authoritarian states such as Russia, China and now Iran (FireEye, 2018, p.3; Giles, 2016, p.3; Giles, 2017; Han, 2015, p.105; Jones, 2018; King, Pan and Roberts, 2013, p.484; Lucas and Pomeranzev, 2016, p.10; (McClintok, 2017; ODNI, 2017[b], p.6; Parliament House of Commons, 2017; Spruds et



al., 2016, p.10; Sullivan, 2014, p.32; Waltzman, 2017). Post Snowden, the *Surveillance and Society Journal* released a series of articles concerning British and American surveillance activities (Garrido, 2015, p. 153 – 155; Keiber, 2015, p.168-170; Schulze, 2015, p.198; Van der Velden, 2015, p.182- 185; Wood, and Wright, 2015, p.132 - 136). However, in response to the Snowden leaks that showed Britain's international propaganda and surveillance measures, little academic attention has focused on GCHQ's propaganda endeavours (Bakir, 2015[a], p.133; Briant, 2015, p.145-146) (see chapter 1).

This is not to imply that no academic scrutiny has been passed, but simply to state that more academic focus is needed to cover an area that has the potential to be a key determining factor to the future of democracy and public opinion in Western democratic nations. To fill this void, I have chosen to focus on the intelligence services of Western governments that have different selves in claiming to apotheosise liberal notions of governance while engaging in similar if not identical propaganda tactics of covert black propaganda and questionable surveillance measures as authoritarian states.

Regardless of how well-rehearsed liberal democratic nations are at distancing themselves from aggressive propaganda and surveillance measures while simultaneously attributing such tactics towards authoritarian states, Western governments engage in dirty tricks at scale. Authoritarian governments such as China, Russia and Iran have openly used propaganda to shape the perception of their citizens. This is not being disputed in this thesis. The point of contention that this thesis aims to overcome is the impression that Western states have a singular self that is democratic and liberal. I assert, particularly in chapter 6, that states have multiple selves which can be bound to both liberal and amoral tendencies. In reality, Western states are keen to employ and make use of propaganda and surveillance within the international arena at scale.

China's recent move to monitor and indoctrinate up to a million Uighur Muslim Chinese citizens while simultaneously using cyberspace platforms for aggressive censorship campaigns throughout its vast population clearly warrants a tremendous amount of scrutiny. However, cyber trolls and online HUMINT that China uses domestically is what GCHQ have decided to use internationally to shape the perception of international disputes (see chapter 1). China's censorship of 1 billion citizens is indeed a repressive

tactic. To some, this may suggest that Britain and the US rank lower as the main producers of propaganda. Coming second third or tenth or twentieth to China is no prize or something to be gleeful about.

If democracies are serious about liberal values, the use of propaganda (by liberal states) to covertly shape the perception of domestic and foreign citizens, to some, should be frowned upon. That is of course unless, liberal values are a part of one particular state ontology or self that is separate from another states sense of self, which is used to fight information wars in the shadows. Britain may not be inculcating its citizens in the same repressive way that China has done with regards to its Uighur Muslim population but, for many decades the UK has engaged in expansive propaganda and surveillance endeavours around the world.

It is crucial to not fall into the orientalist trap of othering states and assuming that a foreign power is morally decrepit while Western liberal nations share no similarities with those they are criticising in regards to propaganda and surveillance measures. For this reason, academics must scrutinise Western countries. A lack of scrutiny itself is near tantamount to censorship, which ironically just so happens to be a form of propaganda. Essentially, Western lies matter too. So do their monitoring programs that cover domestic and international audiences.

In theory, democratic nations should steer clear of malevolent information campaigns that have contributed to the aggrandisement of irrational impulses which paved the way for atrocities throughout the 20th and 21st century. Despite the list of turbulent incidents that propaganda has exacerbated, propaganda continues to be one of the many tools that Western states continue to sharpen for deployment (see chapter 3 and 4). Keeping in line with political rhetoric, Western states are supposed to be a democratic paragon for weak democracies and authoritarian regimes. As announced by former US President Ronald Raegan during the Cold War:

*We've seen such changes in the world in 7 years. As totalitarianism struggles to avoid being overwhelmed by the forces of economic advance and the aspiration for human freedom, it is the free nations that are resilient and resurgent. As the*

*global democratic revolution has put totalitarianism on the defensive, we have left behind the days of retreat. America is again a vigorous leader of the free world, a nation that acts decisively and firmly in the furtherance of her principles and vital interests. No legacy would make me more proud than leaving in place a bipartisan consensus for the cause of world freedom, a consensus that prevents a paralysis of American power from ever occurring again... and as we pray God... that another generation of Americans has protected and passed on lovingly this place called America, this shining city on a hill, this government of, by, and for the people (The American Presidency Project, n.d.).*

Judging from President Reagan's passionate speech, America's effervescent democratic ideals were able to curtail the influence of authoritarianism, thus reinforcing the essence and importance of liberal democratic values. Several decades later, former US President Barack Obama continued with US tradition in asserting that he believes in American democratic 'exceptionalism with every fibre of my being' while failing to comment on the status of over 190 other not so exceptional states (CNN, 2016[a]). Moreover, Britain went to the extent of calling itself Great Britain to emphasise its glory and prosperity, in comparison to other alleged, not so *great* nations. In order for Britain and the US to maintain their sense of ontological self that consists of moral righteousness, publicly distancing themselves from authoritarianism and amoral traits became a key practice.

In reality, Britain's IRD unit monitored public opinion and orchestrated a mixture of white grey and Black propaganda throughout the Cold War in countries such as Malta, Pakistan Uruguay, Guatemala, Norway, Finland, Argentina Switzerland, Iceland Sierra Leone, Ethiopia, Colombia, Panama, Haiti, Lebanon, Fiji, Rwanda, Denmark, Jamaica, Sweden, Canada, Jordan, Australia, Cyprus, Bangladesh, Honduras, India, UK, Zambia, Thailand, Ireland, Persia, Morocco, Mongolia, Kuwait, Qatar, Greece, Chile, Japan, Botswana, Uganda, Kenya, Cuba, Nigeria, Cameroon, Malawi, Tanzania, Bahama's, Cambodia, Mauritius, Burma, Spain, Brazil, Netherlands, Libya, Costa Rica, South Africa, Israel, Congo (Kinshasa) South Vietnam, Bolivia, Paraguay, Algeria, Peru, Bahrain and the US. In the 21st century, JTRIG has targeted Zimbabwe, Russia, Argentina and North Korea with cyber operations comprising of propaganda and surveillance measures.

The CIA orchestrated propaganda campaigns throughout Latin America as well as the FBI's domestic psychological warfare campaign against what it viewed as *Black Extremists* groups (see chapter 3). In the 21st century, the Pentagon hired a British PR firm, Bell Pottinger, to create covert propaganda that was distributed throughout Iraq. Furthermore, the FBI went to the extent of creating a fake terrorist website and leaving an email address in order for the FBI to communicate and ferment its propaganda and incitement of terrorism (see chapter 6).

Modern revelations of US and British propaganda poses fundamental questions about the extent to which democratic governments are truthful about domestic and foreign policy endeavours and the degree to which democratic nations are willing to uphold their values without mimicking authoritarian regimes that President Raegan fought so hard to push back against. The current focus of academics and other researchers seems to be towards (predominantly) authoritarian regimes such as Russia, Iran and China (FireEye, 2018, p.3; Giles, 2016, p.3; Giles, 2017; Han, 2015, p.105; Jones, 2018; King, Pan and Roberts, 2013, p.484; Lucas and Pomeranzev, 2016, p.10; (McClintok, 2017; ODNI, 2017[b], p.6; Parliament House of Commons, 2017; Spruds et al., 2016, p.10; Sullivan, 2014, p.32; Waltzman, 2017).

In the case of Russia, it can be argued that the Kremlin has been operating at a high 'risk threshold' to make it overwhelmingly clear to adversaries that they (Russia) are responsible (Parliament. House of Commons, 2017, p.59). This show of boldness may very well be to underscore and portray Russia's willingness to exert strength in the international arena and highlight its capability to do so at any given time while Western states struggle to overcome the guilt of multiple failed interventions in the 21st century. GCHQ has also stated that China was up until recently not bothered about being attributed to claims of cyber espionage, although this posture is beginning to change (Parliament. House of Commons, 2017, p.61).

China has made considerable efforts to domestically manage public opinion through online propaganda campaigns and keep track of its citizens (Han, 2015, p.105; King, Pan and Roberts, 2013, p.484). Concerned about the threat of public opinion and Muslim

Uighurs citizens in its western province of Xinjiang, Chinese border guards have begun taking phones of visitors to Xinjiang proceeded to download phone applications as a means of keeping track of people (Osborne and Cutler, 2019).

Aside from state concerns about Uighurs and domestic subversion of cultural values, China has been making strides in developing facial recognition technology and advanced AI surveillance equipment to track its citizens. According to Steven Feldstein, China has emerged as a global driver of “authoritarian tech” which emboldens anti-democratic nations to engage in wholesale surveillance of citizens (Feldstein, 2019). With regards to public opinion, the expungement of inflammatory views and video content enables China to keep a finger on the pulse of current trends in cyberspace and to eviscerate popular dissent that poses a threat to Chinese values and the governments grip on power (King, Pan and Roberts, 2013). Government astroturfing is an auxiliary tool the Chinese state uses to help craft an illusion of support and normality amidst its authoritarian rule in the 21st century. Much like GCHQ, perception management is high up on the agenda list of the Chinese government.

Infamously known as the ‘50 cent’ army, China hired Internet commentators (50 cent) to anonymously disperse comments on the Internet in order to drown out views and alter focus on topics to dilute popular dissent deemed to be dangerous (Han, 2015, p.105; Sullivan, 2014, p.32). In contemporary times, Twitter and Facebook have publicly highlighted the issue of individuals linked to the Chinese government or groups backed by China that have engaged in an online propaganda campaign against Hong Kong protestors (Twitter Safety, 2019; Facebook Newsroom, 2019).

During 2019, parts of Hong Kong were inundated with a maelstrom of protests against the local government spearheaded by Carrie Lam and mainland China (South China Morning Post, 2019). Protestors were angry with the Lam’s proposed legislation bill that would have allowed China to extradite Hong Kong citizens to mainland China (Wong, 2019). In response, hundreds of thousands of protestors flooded the streets of Hong Kong, at times in rampant battles with law enforcement and pro-China demonstrations (DW News, 2019). The Chinese government have responded with moving additional military equipment and soldiers to the border with Hong Kong (Wong, 2019). Another measure

by the Chinese government was to launch an information campaign against the protestors (Twitter Safety, 2019). Fake twitter accounts were created to spread propaganda and disparaging remarks against protestors that were angry with the extradition bill (Twitter Safety, 2019).

In August of 2019, Twitter announced that it was aware of a ‘significant state-backed information operation’ that was made up of 936 accounts emanating from China (Twitter Safety, 2019). These accounts were attempting to ‘sow political discord in Hong Kong, including undermining the legitimacy and political positions of the protest movement on the ground’ (Twitter Safety, 2019). Although China’s use of propaganda is of great interest, it is essential to emphasise that this research is based on Western efforts to warp perception online (see chapter 5, 6 and 8) and the overall ontological reaction to modern propaganda efforts by non-state groups (see chapter 7).

Without a doubt, Russia and China have been engaging in propaganda and surveillance activities that are worthy of attention, but not at the cost of suggesting that Western states are unwilling to poison the well with propaganda. This research attempts to bring focus and attention to the behaviour of Western states such as the US and Britain to highlight that the current issue of propaganda is not exclusively a Russian problem or a Chinese problem. Conversely, this thesis will point out the irony of democratic nations avidly convincing themselves and their citizens that they do not produce propaganda. Academic discussion without recognition of Western endeavours is no credible discussion at all. In fact, its expulsion or curtailment can be likened to censorship which is a form of propaganda.

Addressing the paradoxical issue of democratic states that claim to be liberal and orderly when their intelligence services engage in insidious propaganda and surveillance measures (see chapter 1, 3, 6 and 8) is crucial to understanding the difficulty in establishing a liberal Digital Geneva Convention (DGC). Having acknowledged the failure of the League of Nations and to some extent the UN, at trying to replace anarchy with international peace, it is vital to unearth propaganda and surveillance issues that are exacerbated in cyberspace by the US and the UK. Failure to do so will only increase concerns by authoritarian regimes that Liberal states receive preferential treatment and a

curtailed amount of scrutiny. Accusations of preferential treatment is already an existing sentiment of African nations in relation to the International Criminal Court (ICC) cases that have been levelled at African leaders in comparison to Western states that have launched illegal wars in Iraq and Afghanistan in recent memory. Academics must take a brave step forward and provide intense scrutiny towards Western states such as the US and the UK for doing what they have criticised authoritarian states of doing. Unless a weapon in the hand of a liberal state is no weapon at all but merely a shield (see chapter 4).

---

### 1.3 Academic Gap in Knowledge

---

Intelligence services often operate in the shadows behind a veil of secrecy to prevent their adversaries from gaining sensitive information. Although propaganda and surveillance maneuverers have indeed been debated for decades, more research is required to understand the behaviour of democratic Western intelligence services that attempt to warp perception by utilising propaganda and surveillance in cyberspace. Research by Emma Briant, which focused on the evolving propaganda and intelligence methods highlighted the activities of GCHQ (2015, p.145-146).

However, this was not extensive and did not significantly explore the ramifications of development in propaganda technique by intelligence units such as the JTRIG (Briant, 2015, p.145-146). Additionally, Vian Bakir has briefly explored the actions of GCHQ's subunit JTRIG, and their vigorous propagandistic activity in cyberspace (2015[a], p.133). Nevertheless, so far, this research area has not blossomed within academia. It is essential to note that this analysis was also very brief, as was the case of Briant's research.

Similarly, research into 'hybrid trolls' is heavily focused on Russian propaganda activity in Latvia and Eastern Europe, but says very little if anything about Western efforts (Spruds *et al.*, 2016, p.10). Although it is necessary to highlight that, the West was not a part of Spruds and colleagues research remit. At this current moment in time, JTRIG as a search term in Sage Journals produces one result. Coincidentally, the only result was authored by Bakir. Oxford University's Computational Propaganda Research Project (COMPROP) predominantly addresses the automated nature of online astroturfing, also

referred to by NATO as Robotrolling (NATO Strategic Communication of Excellence, 2018). Alternatively, the phenomenon of modern propaganda has prompted the notion that:

*Mass creation of accounts, impersonation of users, and the posting of deceptive content are [behaviours] that are likely common to both spam and political astroturfing. However, political astroturf is not exactly the same as spam. While the primary objective of a spammer is often to persuade users to click a link, someone interested in promoting an astroturf message wants to establish a false sense of group consensus about a particular idea (Ratkiewicz et al., 2011, p.299).*

Accordingly, the COMPROP has a focus ‘of how tools like social media bots are used to manipulate public opinion by amplifying or repressing political content, disinformation, hate speech, and junk news’ (The Computational Propaganda Research Project, 2016). Bots that are of a political orientation can be defined as, ‘algorithms that operate over social media, written to learn from and mimic real people so as to manipulate public opinion across a diverse range of social media and device networks’ (Howard and Woolley 2016, p. 4885). While research by COMPROP has been insightful, much of it is predominantly based on the automated nature of propaganda via bots.

On the other hand, the new wave of online propaganda, at times, is heavily predicated on the use of surveillance, and various tactics. Research papers from the COMPROP have fleetingly mentioned GCHQ and UK’s 77<sup>th</sup> Brigade’s online activity concerning counter-propaganda (Bradshaw and Howard, 2017, p.15). Other than very brief segments of commentary, this paper does not go into detail and explore how such activity may disturb or promote democracy and propaganda practices by Western intelligence services.

Richard Alrich and Christopher Moran believe that ‘[s]cholars now need to interrogate the nature of state secrecy in the United States and the United Kingdom in the early twenty-first century’ in light of the Snowden leaks (Johnson et al., 2014, p.795). In admiration of this point of view, this research is based on probing and inquiring how OS and public opinion is impacted by JTRIG’s playbook and similar modern methods of propaganda and surveillance that are used to warp perception. Postulated back in the early 20<sup>th</sup> century, Harold Lasswell suggested that ‘[t]he rapid growth of specialisation on



propaganda in the modern world is one aspect of the complication of the material and the symbolic environment' (1935, p.189).

In saying this, it is clear that the modern environment has been further complicated by evolving propaganda strategies, thus making it of great importance to dissect and analyse this area of interest. To date, OS as a concept has been appropriated by IR scholars (Johansson-Nogués, 2018, p.528-530; Karp, 2018, p.58-59) but is seldom used as a concept to assess the ramifications of propaganda and surveillance activities that are used to warp the perception of citizens. Furthermore, as mentioned above, the concept of the phantom public has not been applied regularly to modern propaganda practices. Lippmann's lack of faith in modern citizens is relevant to the current era that is permeated with propaganda and surveillance campaigns.

---

## **1.4 What are the far-reaching Implications of Propaganda and Surveillance?**

---

In spite of the fact that propaganda and surveillance has been researched by a litany of scholars throughout the 20th century (see chapter 3 and 4) society is not impervious nor immune from the impact that both phenomena pose, particularly when intelligence services of global powers use them. Propaganda and surveillance are of fundamental importance to the national security apparatus of many states because they are measures that in some cases stop short of an act of war while enabling one state to degrade the influence of another without a bullet being fired. Although cyber-attacks are increasingly being referred to as an act of war or placed in the category of cyberwarfare, it is well known that states are undermining the security networks of allies or rival states. In the 21st century, cyberspace has become a critical battleground for the hearts and minds of citizens around the world. This has forced states to conjure up new ways of monitoring and deceiving people to ensure that the domestic and foreign policy of one state reigns supreme over its rivals (see chapter 5).

Much to the detriment of society, these new means of control can have a destabilising impact on public opinion and an overall sense of OIS concerning public trust in information. Citizens are at risk of developing a strong sense of cynicism and distrust of government officials or non-state groups that spread information. This section endeavours to briefly dissect some of the far-reaching implications of propaganda and surveillance in modern society. For the sake of clarity, this section will be addressed in two parts. The first segment will predominantly focus on surveillance within this current chapter (1.1.3). However, propaganda will be addressed in section 1.1.4. Law enforcement and intelligence services often make use of various surveillance measures to help keep track of criminals. To an extent, modern surveillance methods can play a significant role in deceiving criminals before their arrest. Essentially surveillance can help to set up deceptions that allow law enforcement officials to arrest criminals. On the other hand, the deep-rooted surveillance culture that can develop within a country may create moral conundrums when trying to battle criminal activities online.

During extreme cases of intelligence investigations, a relative sense of morality can become blurred. Child pornography, for example, has become a huge issue primordially due to its expansion on to the dark web. Paedophiles choose to host websites on the dark web to hide their tracks from law enforcement officers that struggle to deal with anonymity in this domain. The dark web can be described as ‘encrypted online content that is not indexed by conventional search engines. Also known as the "darknet," the dark web is a component of the deep web that describes the wider breadth of content that does not appear through regular Internet browsing activities’ (Investopedia, 2019).

When some intelligence services overcome the lack of insight on the dark web and unmask the identities of several paedophiles, analysts may choose to capitalise on information that can help navigate through an unclear terrain. In the case of the FBI and the Playpen child pornography scandal, the FBI took aggressive but necessary surveillance measures to monitor and catch a litany of paedophiles worldwide. However, the FBI’s operation came at the cost of being accused of aiding and facilitating the existence of a child pornography website. What started as a surveillance operation evolved into questions of morality. Excessive surveillance methods, therefore, has the potential to open up deep societal concerns about how intelligence services conduct

sensitive covert operations. Again, it is essential to reiterate that using surveillance to fight crime for the greater good can create a culture of indifference when confronting the partial lack of morality in intelligence work.

In 2014, a foreign law enforcement service informed the FBI about a Tor hidden service called Playpen that was hosting child pornography (Rumold, 2016). Steven Chase created the website on a Tor network that allowed users to anonymously communicate, update and view ‘tens of thousands of postings of young victims, indexed by age, sex, and the type of sexual activity involved’ (FBI, 2017). Once the FBI became aware of Playpen, they were granted a search warrant and seized a copy of the website and took over its server (FBI, 2017). At this point in time, the FBI had a fundamental choice to make; they could either shut down the website or allow it to keep on running. The FBI chose to keep the website running for an additional 12 days to monitor as many visitors as possible (EFF, n.d.).

Cognisant of the fact that this took place in the 21st century, the FBI sent malware to thousands of computers worldwide who clicked on the website (Playpen) in order to track the IP address and identity of those interested in child pornography. This particular method of surveillance enabled the FBI to keep track of paedophiles on a global scale, which reiterates the far-reaching implications of surveillance.

According to EFF, the FBI’s:

*“Network Investigation Technique” or NIT by the government—searched for and copied certain identifying information from users’ computers and sent that information outside of the Tor network back to the FBI in Alexandria, Virginia. Thousands of computers, located all over the world, were searched in this way* (EFF, n.d.).

Back in 2017, Europol announced that ‘368 suspected child sex abusers have been arrested or convicted’ as a result of Operation Pacifier, which was spearheaded by the FBI and assisted by multiple foreign intelligence services throughout the world (Europol, 2017). In fact, the FBI revealed that arrests and law enforcement actions were carried out in nations such as Israel, Turkey, Peru, Malaysia, Chile, and Ukraine (FBI, 2017). To

some extent, surveillance, particularly when it is integrated with child pornography advertisement can cause great moral concern about how Western intelligence services are ensuring national security.

The fact that multiple law enforcement agencies were involved would indicate that multiple nations were aware that the FBI was directly or indirectly hosting child pornography. When contemplating intelligence collection, is it possible that there is a democratic line that intelligence services are unwilling to cross at the risk of allowing criminals to escape? After all, democracies are responsible for their citizens and are duty-bound to protect them from criminals. Conversely, Law professor Elizabeth Joh has refuted the previous rationale in stating that:

*Participating in the distribution of child pornography is a federal crime. But that's exactly what the F.B.I. did in this case... When the government participates in the distribution of contraband, it has little control over who will use those illegal guns, drugs or child pornography, and little ability to protect victims from these harms... In cases like this one, official government participation in crime amounts to a low visibility, high discretion policing tactic with tangible harms. That's the antithesis of policing in a democratic society. The distribution of child pornography is a serious crime. But that alone doesn't justify the government's participation in the crime itself (Joh, 2016).*

Joh has raised a fundamental point in which intelligence services have not sufficiently addressed. How are intelligence services supposed to keep control of vices they produce when engaging in surveillance operations? In other words, when intelligence services create or facilitate propaganda and other vices (child pornography) during surveillance operations, how do they go about controlling the actions of a crazed fanatic or a criminal who might commit heinous crimes before the law can apprehend the individual? On the other hand, chapter 6 demonstrates that the FBI created a fake propagandized terrorist website to attract people and encourage them to commit acts of terrorism in Syria.

---

## 1.5 Propaganda and its Gravity

---

This section attempts to unpack and underscore the significance of propaganda while briefly assessing the implications this (propaganda) can have on democracy and IR. Although propaganda is discussed in great detail in chapter 2, 3, 4, 5, 6, 7, and 8, it is vital to clearly address its significance early on in this thesis as a means highlighting its modern relevance to academia. Although propaganda has been researched significantly, its pervasiveness and gravity continue to grow. The extent to which education has halted the forward march of propagandists to deceive people worldwide is debatable. Think tanks, social media personalities and non-state fact-checkers have all tried to overcome the presence of propaganda during domestic or international debates (Bressan, 2019, Carnegie Endowment, 2019; EU Factcheck, 2019; Good Morning Britain, 2019; Legatum Institute, 2014).

The content and modus operandi of propaganda is polymorphic and rarely ever static or devoid of insightful new *truths*. No matter how ardent a fact-checker may work to find the truth, propaganda finds a way to deceive those that crave simplistic explanations about intricate issues. This issue is compounded further by the difference in perception and ideological adherence among humans. The vicissitudes of human perception have been an immutable experience throughout human history.

Human differences whether it be physical, social, political sexual etc., is a permanent feature that will continue to exist despite attempts made by different groups to convince other citizens, nations or non-state group that one particular economic, political or social way of being is correct. The battle of ideas that takes place in multiple categories may never end. Consequently, information campaigns to shape ideological hegemony may never end. In an attempt to build support for one particular perception, leaders of a particular social faction or nation will employ the use of propaganda. Propaganda can help to reinforce the perception of in-group members at the expense of shattering the ideological crux of opposing groups as a means of mobilising ideological desertion. Desertion need not mean that the ideological deserter must arrive at the propagandist's

in-group, but simply that he or she relinquishes support for an opposing group, thus bringing the overall perception of the *other* into question.

Propaganda can be used to poison the well of information so that people choose to not digest information from any given source or about the controversial topic at hand. The aim of propaganda is not always centred on perception change which creates support for one adversary over the other. An objective of the propagandist may be to overload a debate with claims and counter-narratives so that it becomes hard to know the truth. Consequently, a hostile actor that is poisoning the well of information may pursue its agenda while opposing governments and societies are attempting to distil truth from fiction which may result in cyclical inconclusive debates that do not produce the conviction to respond to aggression. In the 21st century, online trolls, bots and fake news outlets are able to assimilate into people's information diets and sow deceit online, at times, without arousing much suspicion concerning the source.

Moreover, amidst an atmosphere of counterclaims, citizens may become aware of a campaign that only exists to spread propaganda as a result of investigative journalism and governmental intelligence findings. Once people become aware of actors that aim to spread confusion online, citizens can become cynical and distrustful of political debates. Faced with a torrent of potential risks that have permeated modern cyberspace, citizens may perceive their surrounding environment as unknowable and ominous. In this particular cynical frame of mind, citizens might experience OIS and begin to pull away from essential discussions that shape the future of democracy. Consider the following discussion on democracy and cyber propaganda between US radio host Charlemagne Tha God and TV Talk show host Maury Povich. According to Charlemagne Tha God:

*I'm more afraid than anything because I don't know if democracy as we know it is still the same in fact I know it's not... I keep telling everybody to go out and vote next year but what about Russian interference? They're trying to pass election interface bill Mitch McConnell is blocking them (The Breakfast Club 2019).*

Maury Povich responded in stating 'the problem is what we don't know, that's the thing you just don't know. You know you go on social media, who the hell knows who's on

there? I'm confused' (The Breakfast Club, 2019). Fear and confusion from both the above commentators have come into existence because of their knowledge that people are actively trying to fool them, which has brought democracy's survival into question. Social media is supposed to be a liberating platform(s). However, it has been used to shape perception and to freeze public opinion in some cases. This level of cynicism is a threat to democracy if people choose to withdraw from voting as a result of online propaganda and OIS. Propaganda in the hands of a skilled propagandist can lead to extraordinary results that have changed the course of history. 19th and 20th century Europe became infected with the concept of eugenics that strived to create a pure master race at the expense of sterilizing or murdering undesirables in a bid to protect the gene pool of healthy citizens. Acting upon the idea of eugenics was reinforced and justified by propaganda that served to placate any form of dissonance that may occur when contemplating the heinous act of ending someone's ability to spread their genetics further (see chapter 3). Propaganda has the power to make heinous ideas seem logical and beneficial.

Despite the many instances in which humans have failed to resist the urge to inflame societal tensions that lead to violence and discrimination, International institutions such as the UN have struggled to prevent states from using propaganda. The International Covenant on Civil and Political Rights, which prohibits the use of propaganda for war (OHCHR, 2019[a]) has failed to deter states from using overt and covert propaganda during wars. Nations such as Serbia, America, Britain, Russia and others have made use of information to persuade domestic and international observers of their foreign policy aims and the necessity to use force against other states and ethnic groups (Fishman and Greenwald, 2015; ODNI, 2017[b], p.6; 'Prosecutor v. Dusko Tadic aka "Dule"', 1997, p.36; Spruds et al., 2016, p.10; The Bureau of Investigative Journalism, 2017).

Serbia in particular used propaganda to characterise Muslims and Croatians as enemies of Serbians and regularly announced that 'that the Serbs in Bosnia and Herzegovina were in danger and needed to be protected, a need which should inspire Serb members of the JNA to join the struggle to save the Serbs from genocide' ('Prosecutor v. Dusko Tadic aka "Dule"', 1997, p.36). Moreover, in the 21st-century, propaganda in the hands of a skilled propagandist can interfere with the domestic affairs of foreign nations to the

detriment of the foreign policy of a particular target. For example, GCHQ aimed to shape Argentina's perception of the Falkland Islands by using Online HUMINT and cyber operations (Fishman and Greenwald, 2015). When factoring in the knowledge that Britain and Argentina fought a short but bitter conflict over the Falkland Islands, it is clear that hostilities or tension has not entirely dissipated. Rather, the UK have engineered ways to defy the UN Charters decree that prevents states from interfering with the affairs of other nations (Fishman and Greenwald, 201). Propaganda can be used to help accentuate colonial claims to territories in a way that seems logical and natural until leaks reveal that Britain has a hand in shaping the perception of foreign nations. This revelation is dangerous due to the fact that nations other than the UK will make use of similar tactics online once cyber and influence operations become commonplace ideologically and practically (technically). Iran has mimicked GCHQ's online playbook of dirty tricks by creating fake organisations and persona's to spread information online (FireEye, 2018, p.3).

If states are adamant that online dirty tricks are a fundamental tool that can shape international affairs, cyberspace is in danger of becoming a propagandised domain in which nations attempt to shape the affairs of rival nations. This is already a prominent issue in the physical realm considering that intelligence services such as the IRD and the CIA have launched influence campaigns throughout Latin America and colonial Nigeria during the cold war (see chapter 3). Nonetheless, with cyberspace being subject to multiple international campaigns of influence, there are not many places left in which citizens can avoid misleading information. Innocent citizen's that simply want to access truthful content may be subject to the propaganda of foreign powers or in a similarly detrimental scenario become cynical about the threat of foreign interference and choose to disengage from the debate altogether.

Cyberspace has brought an additional issue to the world that increases the gravity and impact of propaganda. Interconnectivity online that reaches a global scale allows for international dialogue between thousands or millions of people which effectively provides a new target for a propagandist to shape. Social media platforms and online news websites such as YouTube, Instagram, Reddit, Twitter, blogs and Facebook can upload information for people to view. With regards to social media companies listed above,



individual citizens can upload information at any given time, which can be viewed by people all over the world. People from across the globe are then able to comment and engage in discussion on any given topic. In essence, cyberspace can create a digital crowd of support or condemnation on past and current affairs.

In the past, the IRD had to find contacts in news outlets in foreign countries to accept its covert propaganda. In contemporary times, this practice may still be used; however, an intelligence service can simply immerse itself within online platforms and begin to shape perception on a larger scale, without the need to potentially comprise any HUMINT sources (Dhami, 2011, cited in *The Intercept*, 2015[a], p.9). The relationship between the propagandist and his/her victim has entered a new stage that is predicated on *real proof* provided in cyberspace that satisfies the curiosity of those who want to see evidence of a scandal. With this upgrade in capability that devolves dependency on traditional news outlets, modern British intelligence services may not be as dependent on journalists to spread propaganda overseas (see chapter 3 and 4). In fact, Iran engages in ephemeral disinformation, a term coined by (Lim et al., 2019) to denote the practice of Iranian actors who create fake journalistic sources and news outlets online, create a following, shape perception then delete the account/ news site and redirect links to a genuine website being impersonated. Similarly, stretching back to 2011, GCHQ sought to upload:

*YouTube videos containing “persuasive” communications (to discredit, promote distrust, dissuade, deter, delay or disrupt)...Setting up Facebook groups, forums, blogs and Twitter accounts that encourage and monitor discussion on a topic (to discredit, promote distrust, dissuade, deter, delay or disrupt)...Establishing online aliases/personalities who support the communications or messages in YouTube videos, Facebook groups, forums, blogs etc (Dhami, 2011, cited in *The Intercept*, 2015[a], p.9) (see chapter 1).*

The point to be made here is that intelligence services are not as dependent on professional journalists to spread false information. Cyberspace provides millions of opportunities for false personas to engage in political debates and shape perception. Intelligence services are thus free to warp perception at scale online, which is a danger to journalism as a profession and most importantly, to citizens that are shaped by propaganda. Moreover,

although perception change may only be temporary until fact-checkers can debunk myths, the contents of ephemeral propaganda may fall into the hands of an unwitting academic, journalist or other prominent figures that can shape perception at scale. To some extent, this scenario would demonstrate how those who shape perception at scale are in danger of consuming propaganda in the same manner as ordinary citizens.

During the recent US impeachment hearing, Fiona Hill warned the Republican Party that they were repeating propaganda lines of Russia's security apparatus (Hill, 2019, cited in CNN, 2019). Since the US 2016 elections, Putin has tried to deflect US accusations of Russian interference by suggesting that Ukrainian Oligarchs had funded Hillary Clinton and that the former Ukrainian President, Petro Poroshenko, wanted to show loyalty to Mrs Clinton (Blake, 2019). On the other hand, during the US 2019 impeachment hearings, Ambassador Fiona Hill stated that:

*Some of you on this committee appear to believe that Russia and its security services did not conduct a campaign against our country and that perhaps somehow for some reason Ukraine did. This is a fictional narrative that has been perpetrated and propagated by the Russian security services themselves (Hill, 2019, cited in CNN, 2019[a]).*

Judging from the above example, some of the most prominent figures within the US Congress have been fooled from a distance yet paradoxically close at home. US National Security Analyst Samantha Vinograd sarcastically highlighted that once upon a time Putin 'paid bots and trolls to spread Russian lies' now Russia can rely on US members of [C]ongress such as Ted Cruz to push claims that Ukraine blatantly interfered in America's 2016 election (Vinograd, 2019, cited in CNN, 2019[b]). Essentially, President Trump and his allies are *useful idiots* that are spreading propaganda unwittingly on behalf of the kremlin but in a way that appears to be in defence of the US and the Republican Party (StopFake, 2017). It is therefore conceivable that academics or other prominent figures who have received information from fake news outlets can inadvertently shape perception on behalf of online actors.

Furthermore, it is worth noting that the battle of information is not exclusive to state actors. Non-state actors have become active in pushing false narratives online. For example, information sharing platforms such as YouTube or Facebook can be used by anyone who has created an account online. Once an account has been created, a child or an adult is able to communicate false information to thousands or millions of people worldwide. The danger that society faces today is that non-state groups have the capacity to malevolently shape hearts and minds at scale. For example, conspiracy theorist Alex Jones often ties unproven conspiracy theories to real blunders and half-truths (PowerfulJRE, 2019).

Of late, Jones appeared on Joe Rogan's YouTube podcast and speculated the agenda behind Eisenhower's public warning about America's military-industrial complex (PowerfulJRE, 2019). After highlighting this revelation, Jones stated that the rejection of the military-industrial complex by President Eisenhower was inspired by his knowledge that NASA had (alleged) plans of becoming a breakaway civilisation that aimed to siphon all the resources from the Earth to build a new advanced system (PowerfulJRE, 2019). Additionally, according to Jones, NASA is bigger than the CIA, spaceships are all a part of "PR" (PowerfulJRE, 2019). Until Jones's recent ban on social media by various platforms for asserting that a US mass shooting was faked by victims families and the government, Jones had one of the biggest conspiracy platforms on social media that attracted millions of views per month (Hafner, 2019; Williamson, 2019). In fact, the families that Jones had accused of faking their own children's death during the US 2012 Sandy Hook mass shooting, received violent threats from strangers (Hafner, 2019; PowerfulJRE, 2019; Williamson, 2019). Clearly, propaganda has far-reaching effects as those who have a good grasp of manipulation can influence people into believing sinister claims online that produce action in the real world.

Often non-state groups act on behalf of states when venturing into propaganda campaigns. Chapter 7 and 8 of this thesis highlights the partnership between states and non-state groups that engage in propaganda and surveillance campaigns. However, in the future, PR companies may choose to exercise their sharpened skills and insights into propaganda to shape the perception of foreign countries independent of intelligence services.

So far, this form of propaganda has not matched the horror or scale of destruction as Nazi Germany or the scale of China's indoctrination of Uighur Muslim citizens. To some, the issue of propaganda is not one worthy of mention because modern citizens are more educated and therefore unlikely to replicate the horrors witnessed in Nazi Germany. So, why is this issue worthy of additional research? The veracity of an argument concerning the impact of propaganda cannot be solely based on how many dead bodies have piled up as a result of cyber propaganda. Rather, I implore readers to contemplate the impact that cyber propaganda can have on the sovereignty of the state, human rights, OIS and the scale of confusion that can evolve into vacuous yet believable conspiracy theories.

Instead of reducing propaganda to increase public trust, states are eager to secure their share of influence online for fear that their narrative will be crushed and ridiculed by an adversary who does not wish to discontinue its campaign of deceit. And so the wheel continues to turn, with the only real consistent losers being citizens who are at the mercy of propagandists they cannot see, nor directly convince to put an end to their covert dirty tricks. Although fact-checkers do exist, stopping the vast torrent of information is a feat that may not be accomplished. Surveillance is a fundamental tool that has enabled the creation of sophisticated influence campaigns which poses a great threat to the democratic values of Western liberal societies. Overall, regardless of whether propaganda and surveillance are evaluated in unison or separately, both tools are of great use to the state, but this comes at a great cost. The issues discussed in this chapter will be covered in greater detail in chapter 3, 4, 5, 6, 7 and 8.

---

## 1.6 The State and Private Companies participation in Propaganda and Surveillance

---

This thesis will focus mainly on the actions of intelligence services that operate at the command of sovereign states. The rationale behind focusing on the state is predicated on the ethical and ideological concerns that are bound to the use of engaging in covert propaganda and surveillance campaigns. Nations often present themselves as rational, peaceful and in the case of democracies, liberal. Western democracies such as the US and the UK who play integral positions in managing global security must contend with the issue of defeating external threats in an international system that at times does not regulate hostile actors. As a result, global powers take decisive measures to curtail the capacity of other states. Such measures, i.e. propaganda and surveillance, are useful tools that states will use to understand and counter the threats posed by their adversaries. However, such measures are often imbued with amoral contents and consequences that contravene the social, ontological and legal fibres that Western democratic states claim to be beholden to. Throughout the 20th century, this dichotomy has been largely unresolved.

The US and the UK have used covert propaganda and surveillance tactics or dirty tricks to shape domestic and external affairs throughout the world. Much to the detriment of America's democratic spirit, the CIA bombed churches in Ecuador as a means of stimulating animosity towards left-wing groups (Blum, 2003, p.173). Moreover, the British IRD released black propaganda throughout Latin America and its former colonial possessions in Africa to thwart communist ideation, despite the UN Charter's opposition to foreign interference (TNA: CO 1035/117). The hydra of security threats continued to grow into the 21st century in which British and American efforts have adapted technologically to spread greater influence throughout the world.

However, the greater the capacity that these states have to overrule the UN Charter's prohibition of interference in domestic affairs, in conjunction with the continuation of claims that Western democracies are liberal and peaceful; the greater the concern that academics should have about Britain and America's actions within the international

arena. Prior to this thesis a great amount of academic attention was provided towards the NSA and GCHQ in a post-Snowden environment (Fidler, 2015, p.200; Greenwald, 2014[b], p.108; Lyon, 2014[b], p.2; Masco, 2017, p.397). However, the same level of attention and scrutiny was not provided to states such as the US and Britain that use propaganda and surveillance techniques, at times concurrently, to shape perception domestically and abroad. For these reasons, I have chosen to focus on states. For the sake of clarity, I have chosen to focus on Western states because of their admiration for liberal values that struggle to keep a pace with the desire to engage in morally questionable propaganda and surveillance campaigns.

Authoritarian states are often characterised as harbouring impulses that leads to reckless actions within the international arena. Liberal Western states have convinced themselves that they have left their decrepit ways in the annals of colonial and pre-colonial history. This is anything but the case. Liberal Western states use dirty tricks in similar ways that their adversaries do. What is troubling is society's ability to ontologically hit a reset button and wipe clean the memory of previous violations while highlighting the use of dirty tricks by another state such as Russia or China.

This thesis will demonstrate that Western states are willing to warp perception online to meet domestic foreign policy goals. From this viewpoint, Western liberal democracies have been stuck at a precipice of completely mimicking its adversaries tactics. On the other hand, perhaps it is the other way around. Nonetheless, the democratic fibre of Western states cannot continue to be tarnished with the statins of vices of dirty tricks without the risk of plunging faith in institutions and the state. Academic scrutiny is therefore required to help steer adverse consequences away from society. When analysing surveillance practices, this thesis will be predominantly focused on assessing surveillance at the state level. Surveillance is undoubtedly carried out by the state at a considerable level. The Snowden revelations demonstrated that the US, UK, Canada, New Zealand and Australia work together to spy on world leaders, companies and citizens.

The scale at which Britain and America were engaging in wholesale surveillance forced both countries to change their laws amidst a barrage of legal battles from NGO's such as Liberty and Privacy International. Two years after the Snowden revelations, US Congress

passed the United States of America (USA) Freedom Act 2015 to bring about a halt to the bulk collection of domestic phone records that were implemented under section 215 of the US Patriot act after the 9/11 attack in New York (Human Rights Watch, 2016; Congress (US), 2015). Similarly, the UK has passed the 2016 Investigatory Powers Act (IPA) with alleged greater safeguards, although of late the UK has lost a court case due to the inadequate provisions and regulations that lead to abuses by MI5 (BBC, 2019[a]; Bond, D. 2019).

In addition, states do not always carry out propaganda and surveillance campaigns by themselves. At times nations will use non-state groups to help mask their digital tracks or simply to help do a better job. It is vital to highlight the role that is played by non-state groups that can store process and manipulate a significant amount of data that originates in dozens of countries around the world. Private companies take part in the collection, aggregation and manipulation of data. In recent years companies such as Palantir have attracted scrutiny for its advanced capability to store vast amounts of information and provide deep insights (Frank, 2018; Waldman Chapman and Robertson, 2018). Palantir's products are used by governments and intelligence services to bolster national security objectives. During America's war in Iraq and Afghanistan, Palantir worked in association with the Pentagon and the CIA. Information that is fed into Palantir's solutions helped to make connections that were used to assist in tracking insurgents and avoid roadside bombs (Waldman, Chapman, and Robertson, 2018). In previous years Palantir's CEO Alexander Karp has suggested that its products can benefit intelligence analysts that are attempting to catch terrorists rather than engaging in something sinister. According to Karp:

*Palantir Technologies has designed what many intelligence analysts say is the most – effective tool date, to investigate terrorist networks. The software's main advance is a user-friendly search tool that can scan multiple data sources at once, something previous search tools couldn't do. That means an analyst, who is following a tip about a planned terror attack, for example, can more quickly and easily unearth connections among suspects, money transfers, phone calls and previous attacks around the globe (Karp, 2011).*

In addition, Palantir has been able to cite examples to which their products have been of great use to national security in spite of the fact that they engage in the collection and surveillance of vast swaths of information. In the aftermath of Hurricane Florence that destroyed large parts of North and South Carolina in 2018, a voluntary military organisation called military veteran volunteer corps Team Rubicon sought to help those on the ground that were greatly impacted by the natural disaster (Palantir, 2019). Team Rubicon employed Palantir's Gotham solution to help coordinate and execute six search and rescue operations by conflating publicly available flood data, weather reports and 'social vulnerability census data to find the communities in greatest need' (Palantir, 2019). Content with the success of Gotham after Hurricane Florence, Palantir has maintained the view that their product helped those that were in dire need of assistance (Palantir, 2019). Framed in this way, it becomes harder to label and position Palantir as being a detriment to human life and cyberspace (Palantir, 2019).

However, Karp's above statement appears to be fairly innocuous at first hand. On the other hand, a regular theme in this thesis concerns the abuses of technology that allows for the surveillance and manipulation of data. Keeping abreast with the former issue concerning the surveillance of data, it has been reported that JP Morgan was allegedly forced to remove its own head of special operations Peter Cavicchia because he was using Palantir's products to spy on JP Morgan's executives (Frank, 2018). In 2009, JP Morgan had engaged Palantir's technology to aggregate data in the search for patterns that would help unearth rogue workers and threats to the company. Cavicchia's special operations team capitalised on the collection of:

*[E]mails and browser histories, GPS locations from company-issued smartphones, printer and download activity and transcripts of digitally recorded phone conversations. Palantir's software aggregated, searched, sorted, and analysed these records, surfacing keywords and patterns of behaviour (Waldman, Chapman, and Robertson, 2018).*

After much success, Cavicchia went Rogue and began monitoring executive's phone calls (Frank, 2018). As a result, colleagues would start planting false information as a trap to see if Cavicchia would bring this up at meetings which allegedly took place (Waldman



Chapman and Robertson, 2018). On the other hand, in some scenarios, it is difficult to determine if the state is behind the activity of state groups or in fact, posing as non-state groups. According to Blum, the CIA would create organisations in Ecuador to construe social and political dissent throughout society (1986, p.171).

To the world, this is a non-state group independent of state direction, thereby solely responsible for any information or violence that takes place. Fast forward to the 21<sup>st</sup> century, this practice still happens. For example, according to the Office of the Director of National Intelligence (ODNI) report on Russia's alleged 2016 US election interference, Russia's military intelligence unit, the GRU, 'used the Guccifer 2.0 persona and DCLeaks.com to release US victim data obtained in cyber operations publicly and in exclusives to media outlets and relayed material to WikiLeaks' (2017[b], p.8).

Similarly, research by cybersecurity vendor FireEye has suggested that Advanced Persistent Threat 28 (APT28) is sponsored, controlled and used by Russia to hack into systems to steal data and leak information through 'the use of "false hacktivist personas," including, among others, "CyberCaliphate," "Guccifer 2.0," "DC Leaks," "Anonymous Poland," and "Fancy Bears' Hack Team"' (FireEye, 2017, p.3). Regardless of what shell is used by a state, in hindsight, this still appears to be state actors directing affairs. On the other hand, APT 34 is believed to be a threat group that is 'backed' by the North Korean regime and conducts cyber financial crime on behalf of the regime (Fraser, et al., 2018).

This would appear to suggest a dividing line between control and support. It is difficult to quantify the full extent to which states employ non-state groups to do its bidding. Aside from extrapolating present and future possibilities concerning the number of times states use non-state groups to conduct dirty tricks, the use of mercenaries has been used by democratic and authoritarian states for centuries. Throughout the 20<sup>th</sup> century, both Britain and America supplied information to media outlets and other institutions in order for recipients to spread information further throughout Nigeria and Latin America (see chapter 3).

Additionally, during the second Gulf War, America used a PR firm, the Lincoln Group, to translate and place pro American stories in Iraqi news media (Mazetti, and Daragahi,

2005). Again, it is crucial to point out that it is not just authoritarian states that use this method of dirty tricks. Democracies, as well as authoritarian states, are willing to poison the well, to win the battle of information regardless of how covert and misleading their tactics may be. This particular talking point is crucial to chapter 7 as the non-state group CyberBerkut waged a propaganda and surveillance campaign to discredit an anti-Russian journalist, potentially at the behest of Russia (Hulcoop et al., 2017).

Unsurprisingly, chapter 8 is predicated on the Pentagon's use of PR firm Bell Pottinger to create dramatised propaganda videos in a bid to punctuate support for Al-Qaeda in Iraq (The Bureau of Investigative Journalism, 2017). Both chapters seek to explore the ramifications of combining state and non-state efforts to warp perception online.

Furthermore, popular tech companies whose services are used by hundreds of millions of people worldwide also play a role in shaping perception and the monitoring of data. Companies such as Twitter and Facebook permit users to communicate and share information with each other around the world. Algorithms can be used to track what users have an affinity to search and watch on their platforms. In this respect, Google and other search engines can also track and aggregate search queries. Additionally, apps on smartphones collect information from the mobile device, such as email address, geolocation, name, etc., which is sold on to 3<sup>rd</sup> party companies for advertisement purposes.

Besides advertisements for monetary gain, tech companies play a pivotal role in shaping and enhancing political propaganda during election campaigns (The Guardian, 2018). Accusations by US Republican senators such as Ted Cruz and Mike Lee that Facebook and Google suppress conservative information online has raised concerns about the role tech companies can play in shaping perception of millions of people worldwide (Shepardson, 2019). Moreover, in 2018 the Cambridge Analytica scandal sent shockwaves throughout the world (European Parliament, 2018; Schroepfer, 2018). Cambridge Analytica is a British political consulting firm which used data mining tactics to help clients target information to change societal attitudes towards the client.

Whistleblower Christopher Wylie came forward with damning revelations in 2018, highlighting how Facebook user data was being used to target people online during elections. Beginning with Facebook's account of events, it came to the attention of Facebook back in 2015 that a psychology professor, Dr Aleksandr Kogan, had violated its platform policies. Dr Kogan began 'passing data from an app that was using Facebook Login to SCL/Cambridge Analytica, a firm that does political, government and military work around the globe' (Grewal, 2018). Kogan had created an app; 'thisisyourdigitallife' that tested the personality traits of its users, which was downloaded by 270,000 people. The app requested access to information such as 'the city they set on their profile, or content they had liked, as well as more limited information about friends who had their privacy settings set to allow it' (Grewal, 2018).

Kogan had gained access to those who downloaded the app and the data of their friends which quickly scaled into the millions (Lapowsky, 2018). Facebook has conceded that the information of up to 87 million people may have been improperly shared with Cambridge Analytica (Schroepfer, 2018). As a result of this harvesting campaign, Cambridge Analytica used the information to target people with political ads that often turned out to be propaganda. One of Cambridge Analytica's most prominent clients was the Donald Trump presidential campaign (Cadwalladr, 2019). However, the same harvesting techniques were used by a Canadian based tech company, AggregateIQ, which was set up by Cambridge Analytica (The Electoral Commission, 2019; Cadwalladr, 2019). The UK Vote Leave campaign, which was the main pro Brexit campaign body during the 2016 referendum used AggregateIQ to harvest data and engage in targeted online campaigns to persuade people to vote to leave the EU (The Electoral Commission, 2019; Cadwalladr, 2019).

In doing so, the UK Electoral Commission announced that Vote Leave broke electoral campaign rules because money was diverted to a youth group named *BeLeave* which was then channelled to AggregateIQ (The Electoral Commission, 2019; Cadwalladr, 2019). The issue at hand is that on two occasions in recent memory, the data of millions of people was misused by non-state groups that did not result in severe penalties by regulatory bodies in the UK and the US. Targeting people's impulses has been a prominent theme

within the advertisement industry for decades. In the case of Cambridge Analytica, information was harvested without the knowledge of Facebook users.

However, the most chilling aspect of both scandals is the ability of companies to advance the interests of individuals or groups during an election by targeting citizens with ads that they may find hard to resist. In effect, the Cambridge Analytica approach could be perceived as attempting to enclose citizens with information online that is relevant to the goal of the client. Although this may not be viewed unequivocally as censorship when one opponent can drown out the information of others and present ads that are favourable to them, the individual citizen is being shaped predominantly by a limited amount of information sources. Furthermore, keeping a pace with the technological change and forcing leading tech companies to face government and public scrutiny to gather key information has been an issue with regulators in the UK. Mark Zuckerberg refused to turn up to UK parliamentary committees, provoking MP's to assert that:

*By choosing not to appear before the Committee and by choosing not to respond personally to any of our invitations, Mark Zuckerberg has shown contempt towards both our Committee and the 'International Grand Committee' involving members from nine legislators from around the world (Parliament. House of Commons, 2019, p.16).*

To a great extent, state control and influence over tech giants is capricious and not necessarily as straight forward as assuming that non-state groups are consistently subservient groups that represent nothing more than a tool for powerful egoist nations. From this angle, the discussion on Realism may be fundamentally flawed in its assumption that non-state groups cannot influence state decisions and IR. In addition, private companies have the capacity to vacuum up vast swaths of data to turn over a profit at the expense of privacy for millions of people. Digital rights, or the digital right to privacy as highlighted by the UN was clearly violated in the above example. The question for future researchers to ponder is; how can other non-state liberal institutions leverage enough control to protect user data without breaking up big tech firms? US presidential candidate Elizabeth Warren intends to break up Facebook; however, this may be a step

too far to the left considering that millions of people still choose to use Facebook despite recent scandals (Stevens, 2019).

In the future, Warren's audacious plan may become more appealing as tech companies struggle to deal with disinformation campaigns, live-streamed terror attacks and highly targeted disinformation ads on their platforms which are not being combatted quickly enough. Germany, on the other hand, has passed legislation that enables the government to fine social media companies up to €50,000, 000 for not (quickly) removing hate speech, fake news and illegal material (BBC, 2018[a]; Echikson and Knodt, 2018, p.3). In slight contrast, Facebook announced that it would not regulate political speech on its platform. Nick Clegg, the current Vice President of Facebook's Global Affairs and Communications, made a stunning admission in stating that:

*We have a responsibility to protect the platform from outside interference, and to make sure that when people pay us for political ads we make it as transparent as possible. But it is not our role to intervene when politicians speak. That's why I want to be really clear today – we do not submit speech by politicians to our independent fact-checkers, and we generally allow it on the platform even when it would otherwise breach our normal content rules (Clegg, 2019).*

Regardless of how outlandish and foolhardy this decision is, it demonstrates the current difficulty that liberal institutions have to embrace when attempting to establish digital freedoms and the right to truthful information. If private companies are unwilling to regulate state figures and their platform when politicians are clearly making erroneous claims, it becomes hard to set a moral standard for citizens who wish to do the same thing. Senator Warren sarcastically emphasised the gravity of regulating political ads worldwide in deciding to sponsor an ad which falsely claimed that Zuckerberg had endorsed President Trump. The ad stated; ““Breaking news: Mark Zuckerberg and Facebook just endorsed Donald Trump for re-election”” (Newburger, 2019). Without a common perception of morality that can be applied on a broad international scale, attempts to regulate Facebook and other tech companies are hopeless and fundamentally flawed from the beginning. Propaganda and surveillance will essentially be left to change its shell and

manifest in different forms with citizens being the ones who are the victims of rogue states and tech companies.

The role of non-state groups in conducting propaganda and surveillance campaigns will be highlighted and explored in different stages of this thesis. Although non-state groups play a significant role in chapter 5, 7 and 8, the predominant focus will be on the state. In 3 case studies, non-state groups were used by the state to conduct propaganda and surveillance activity. In the case of chapter 8, British PR firm Bell Pottinger was used to help create covert psychological warfare products on behalf of the Pentagon and US Generals on the ground in Iraq.

Similarly, in chapter 5, WikiLeaks released stolen information allegedly on behalf of the Russian Government to disrupt the US 2016 election (ODNI, 2017[b], p.12-13). How states should respond to non-state groups being used to further foreign policy agendas of adversaries is haphazard and unclear (The Bureau of Investigative Journalism, 2017). In the case of WikiLeaks's role in releasing the GRU's stolen information from the DNC, the Trump campaign defended WikiLeaks's right to share information that they had not stolen. Cited from *Roy Cokrum V Donald J. Trump for President*, according to the Trump campaign:

*Under section 230 of the Communications Decency Act... a state may impose liability on "the original culpable party who posts [tortious] messages," but not on "companies that serve as intermediaries for other parties' potentially injurious messages." ... As a result, a website that provides a forum where "third parties can post information" is not liable for the third party's posted information... Since WikiLeaks provided a forum for a third party (the unnamed "Russian actors") to publish content developed by that third party (the hacked emails), it cannot be held liable for the publication ('Roy Cokrum, ET AL. v Donald J. Trump for President' 2018, p. 18).*

In accordance with the doctrine cited above, US news outlets have been releasing leaked information for decades. According to US Republican Senator Ron Johnson between January 20 and May 25, 2017 'at least 125 stories with leaked information potentially

damaging to national security’ were displayed by US national news organisations. (Johnson, 2017, p.2). However, releasing damning revelations about the state is crucial to keeping the government in check and preventing the democratic slide into authoritarianism. If the USG were to indict WikiLeaks for its role as an alleged Russian auxiliary tool during the US 2016 election, the current President of the USG may be setting a dangerous precedent that would ultimately prohibit the press from highlighting instances when states go rogue, thereby silencing the free press.

On the other hand, when journalists knowingly persuade government officials to break their oath and legal duties of keeping information safe, it could be argued that this is just as bad as a non-state group who simply acted as an intermediary by receiving information and sharing it online. Yet, major news outlets continue to publish information they have gathered from internal government sources. Conversely, when non-state groups break the law by physically or electronically stealing information as opposed to convincing a government source to hand over information willingly, the hostile actor cannot be defended by stating that one only shared information by uploading data online. US Secretary of State Mike Pompeo referred to WikiLeaks as a ‘non-state hostile intelligence service often abetted by state actors like Russia’, partly because WikiLeaks conspired with Chelsea Manning to carry out the ‘the largest compromises of classified information in the history of the United States’ ( US Department of Justice, 2019; Pompeo, 2017).

According to the US Department of Justice’s 2019 Indictment charge ‘Assange conspired with Manning; obtained from Manning and aided and abetted her in obtaining classified information with reason to believe that the information was to be used to the injury of the United States or the advantage of a foreign nation’ (US Department of Justice, 2019). Consequently, Assange has been indicted on 18 counts as a result of ‘Illegally Obtaining, Receiving and Disclosing Classified Information’ back in 2010 (US Department of Justice, 2019). Judging from the language used by the US Department of Justice, it would appear that receiving and obtaining information is a crime, thus leaving a legal grey area about how to deal with domestic news outlets that publish information.

In addition, it remains unclear how states and institutions are supposed to sanction companies that create propaganda on behalf of a state. US Psyops that is designated for

foreign consumption is a longstanding practice (Paul, 2010). If the US chose to leverage Psyops endeavours to a private company, it is not much different than the USG hiring ‘Private Security Contractors... to protect individuals, transport convoys, forward operating bases, building’ and assist in training Iraqi police and military personnel during the second Gulf War and private military companies that fought on behalf of the US in Afghanistan (Elsea Schwartz and Nakamura, 2008, p.2). When portrayed in this manner, nothing seems overwhelmingly suspicious.

On the contrary, this thesis highlights instances in which grey and black propaganda are produced by private companies on behalf of the state. Non-state groups are not entirely impervious to the reality of their potential role in producing dangerous information. The disgraced UK PR firm Bell Pottinger has been entrenched in multiple scandals for producing insidious and dangerous information.

Beyond Bell Pottinger’s work for the Pentagon, a leaked email has revealed the role it played in producing racist propaganda in South Africa for private interest groups (Maclean, 2017). In this instance, Bell Pottinger did not produce propaganda for another state. However, the information was used in another country. As a result of the indignation felt in the former apartheid state, the South African Democratic Alliance lodged a complaint with UK based regulators, the Public Relations and Communications Association and the Chartered Institute of Public Relations. Consequently, the Public Relations and Communications Association removed Bell Pottinger from its membership highlighting that “‘Bell Pottinger has brought the PR and communications industry into disrepute with its actions, and it has received the harshest possible sanctions’ (Ingham, 2017, cited in Public Relations and Communications Association, 2019; Van Damme, 2017).

Since this announcement, Bell Pottinger has suffered reputational damage which triggered resignations, an investor exodus and the eventual closure of its UK based holdings. It is important to note that these regulatory bodies are not a part of the UK government. Membership to both regulators is a symbolic indicator of a certain standard. The legal implications of Bell Pottinger’s various dealings or any non-state group for that matter will be subject to the laws of a nation that any given company is operating in.



To a great extent, there are not many places left in this world in which an individual can say with confidence that they are not being monitored or that their information is not going to be exploited in a nefarious way or at least in a manner that they were unaware of. Although the state plays a pivotal factor in this ominous picture, non-state groups have an increasing role to play in the erosion of privacy and an increase in the aggregation of personal data. Cognisant of the UN's right to digital privacy resolution, it becomes difficult to understand and perceive how non-state groups and states will forge a memorandum of understanding or a binding international agreement that will bring an immediate or gradual end to propaganda and surveillance measures which will satisfy privacy advocates. Human rights or digital rights seems to be held hostage by state and non-state desire to engage in self-help practices ironically much at the detriment of those they are trying to protect (Blanton and Kegley, 2017, p.24).

Effectively, Becks concept of a *Risk Society* or a digital freedom risk environment, is being greatly aggrandised in the digital sphere by two predominant groups, i.e. the state and non-state groups such as tech companies (2016, p.141). With greater visibility into the lives of consumers and citizens, society is sleepwalking into a digital catastrophe where significant portions of our lives are digitised and subject to digital manipulation for the benefit of financial gain and geopolitical interests.

---

## 1.7 Propaganda and Surveillance: Two Sides of the Same Coin

---

Ordinarily, propaganda and surveillance are seen as two separate subject areas due to the perception that the former and the latter are intrinsically different. To an extent, this assumption is correct. Surveillance consists of intermittent or persistent monitoring of humans, while propaganda is an event or form of communication designed to influence the perception of a desired set of targets. Depending on the perspective of any given author, propaganda and surveillance may be taught separately within Communication Studies, Sociology, Psychology, IR and other research fields. Conversely, I have chosen

to analyse propaganda and surveillance concurrently throughout this thesis. Propaganda and surveillance are two sides of the same coin.

Intelligence services and non-state groups, aggressively search for information in the physical world and cyberspace to exploit, in order to have an impact on domestic citizens or foreign nations. Often, propaganda and surveillance complement each other and provide a basis for successful social and political endeavours. Organisations such as the CIA and GCHQ, recognise the necessity of using both propaganda and surveillance concurrently or in close coordination with one another despite their remit predominantly focusing on the collection of intelligence.<sup>3</sup>

In the past, monitoring, obtaining and exploiting information was integral to the CIA. This was particularly evident during the CIA's pursuit to capitalise on the Khrushchev speech. In 1956, Khrushchev made a ground-breaking secret speech to the Communist Party of the Soviet Union. Khrushchev's speech delegitimised Stalin's 'cult of personality' which allowed him (Stalin) to distort Lenin's ideology and the general communist movement (Wilson Center, 1956, p.1). At the start of the speech, Khrushchev highlighted Lenin's open desire to have Stalin replaced with someone with 'greater tolerance, greater loyalty, greater kindness, and more considerate attitude toward the comrades, a less capricious temper' (Wilson Center, 1956, p.2-3).

Similarly, Khrushchev reviewed Stalin's habits and reminded the audience that '[w]hoever opposed this concept or tried to prove his viewpoint, and the correctness of his position was doomed to removal from the leading collective and to subsequent moral and physical annihilation' (Wilson Center, 1956, p.3). Circulation of this speech was scant as the Soviet Union feared that the denouncement of Stalin would cause ideological and literal agitation amongst communists in Europe. However, the CIA became aware of the speech and decided to press operatives and contacts to ascertain a copy in order to sway public opinion and incite agitation throughout communist-dominated territories. Moreover, Amos Manor, the former head of Israel's intelligence service, Sin Bet, received a copy of the speech from a Polish Journalist in an Israeli embassy located in

---

<sup>3</sup> Indeed the CIA has a sizable remit for intelligence collection, but it is important to note that after WW2 this scope expanded to Covert Action which included sabotage in NSC-4A see <https://history.state.gov/historicaldocuments/frus1964-68v12/actionsstatement>

Warsaw (Melman, 2007). Manor delivered the speech to the CIA, to which the head of the CIA, Allen Dulles, shared the speech with the Eisenhower administration (Melman, 2007; Office of the Historian, n.d.[a]). Once a copy of the Khrushchev speech was in the hands of the CIA, an ‘intense argument’ took place at the CIA with regards to what to do with the speech (Ranelagh, 1987p. 287).

At the time, Ray Cline, a former CIA analyst, pleaded for the speech to be made public in full to ‘provide scholars and students... invaluable insights into the real workings of Stalinist Russia’ and to confirm what the US had already been saying about Russia (Ranelagh, 1987, p. 287). Conversely, according to John Ranelagh, senior CIA staff such as Frank Wisner and James Angleton refuted Cline’s view and ‘proposed that the speech be exploited by feeding selected bits of it to particular audiences in order to create a specific impact’ which was unrest in eastern and central Europe (Ranelagh, 1987, p. 287). In the end, President Eisenhower gave permission for Dulles to release the speech to the press (Office of the Historian, n.d.[a]).

Subsequently, the speech was released to the New York Times, which caused a political crisis throughout communist-dominated territories in Eastern Europe (Ranelagh, 1987, p. 288). This example demonstrates that intelligence services coordinated surveillance (operatives) to retrieve information that is used for propaganda purposes of swaying public opinion in foreign territories. In this example, it is self-evident how the careful release of information can have a negative cascading effect in multiple nations. In contemporary times, this process has been digitised. Intelligence services or non-state actors exfiltrate vast amounts of information and edit them with sophistication to pass edits off as real documents. Additionally, a propagandist may choose to release information online in a similar fashion as the CIA did. Only this time, the perpetrator can inflame societal divisions within online platforms in order to have the desired goal of warping perception.

Leaked documents have revealed that GCHQ’s subunit, JTRIG, wielded both propaganda and surveillance measures to influence cyberspace. According to the Snowden leaks, JTRIG provides GCHQ’s online influence capability, e.g. propaganda or information

influence in addition to some of its surveillance capability (Dhami, 2011, cited in The Intercept, 2015[a], p.5). One of JTRIG's main core functions consists of '[a]ctive covert internet operations (including online HUMINT and effects)' (Dhami, 2011, cited in The Intercept, 2015[a], p.5). For example, online effects consist of:

*'[E]stablishing an online alias/personality who has a Facebook page, and membership of relevant web forums... Interactions with the target may be informed by a combination of analysis of SIGINT provided by the IPTs, monitoring of the target's online behaviour, and intelligence from SIS'* (Dhami, 2011, cited in The Intercept, 2015[a], p.9-10).

Clearly, GCHQ understands the necessity of using surveillance material to improve propaganda products. Therefore, it is not an outlandish notion to view propaganda and surveillance simultaneously or in close coordination with each other. However, I maintain the view that both propaganda and surveillance complement each other and needs to be assessed as two sides of the same coin at various junctures throughout this thesis.

---

## 1.8 Walter Lippmann and the Phantom Public

---

Lippmann would be amazed to see how far propaganda has come in the 21<sup>st</sup> century considering the development of Deepfakes, Hybrid Trolls and ephemeral propaganda methods that are becoming an issue for citizens to decipher and governments to combat (Dack, 2019; Langston, 2017; Wakefield, 2018; Spruds et al., 2016, p.10; Suwajanakorn, Seitz and Kemelmacher-Shlizerman, 2017, p.1-3; Lim, et al., 2019). No international sovereign body exists that can restrain states and non-state groups from engaging in propaganda which leaves citizens exposed to a litany of propagandists. In the build-up to the second Gulf War, the world was misinformed about Saddam Hussein's alleged Weapons of Mass Destruction.

This eventually led to the illegal invasion of Iraq. Moreover, the positive reaction that President Trump has received from his *base* of supporters for launching relentless attacks on political rivals and Mexicans (and Latin Americans in general) has demonstrated how

propaganda can be welcomed in society. In spite of the fact that the world witnessed countless amounts of horrors in the 20<sup>th</sup> century that were aided by propaganda, this phenomenon is paradoxically repudiated by some and welcomed by others. Lippmann's concept of the phantom public dates back to the 1920s but its implications are still relevant. This section endeavours to highlight the extent to which Lippmann's term, the phantom public is relevant to modern society. To reiterate, Lippmann claimed that Citizens do not have:

*Opinions on all public affairs... he does not know what is happening, why it is happening, what ought to happen. I cannot imagine how he could know, and there is not the least reason for thinking, as mystical democrats have thought, that the compounding of individual ignorance's in masses of people can produce a continuous directing force in public affairs (Lippmann, 1993, p.29).*

Propaganda offers quick explanations for complex issues which helps to ease the cognitive load that requires a citizen to understand the various intricacies of domestic and foreign affairs. British Prime Minister Boris Johnson has repeatedly peddled simplistic slogans such as 'get Brexit done' in a bid to curtail the complexity of leaving the EU without delivering a crippling blow to the British economy (Rawnsley, 2019; ITV, 2019[a]). The stark potential reality of Brexit has, to some extent, been obfuscated by Conservative *Brexiters* and replaced with propaganda. For example, the infamous *pink bus* that was used by the then MP (Boris) Johnson to suggest that an extra £350,000,000 would be added per week to fund the NHS if the UK left the EU is one of many examples of fanciful assertions made that turned out to be propaganda (ITV News, 2019[b]). Post-Brexit, former Prime Minister Theresa May was presented with the following question which highlights the impact of propaganda that encouraged voters to vote to leave instead of reviewing the full implications of Brexit:

*Theresa May could you please justify to me why I have leaflets saved at home delivered to me by local conservatives before the EU referendum stating clearly that we will save £350, 000, 000 million per week for the NHS if we leave the EU. That lie is the only reason why I and I'm sure many others here tonight possibly decided to vote leave? (Liberal Democrats, 2017).*

Fundamentally, the Conservative government's response to the issue of Brexit along with the leave campaign, which has been to push inaccurate and fanciful outcomes (that was primarily received by pro-leave voters) is evidence that some voters, however large or small, may appreciate this form of digestible and straightforward information. Belief and admiration for propaganda produced by the Conservative Party have occurred partly because its content is partially true; or quite possibly because the Conservatives have offered a delusional but simplistic approach that assimilates seamlessly with preconceived ideas and wishes of the constituents that voted for Brexit. According to Brexit voters that were interviewed at random by The Guardian back in 2016, one voter suggested that she wants the borders regulated because rape, child deaths and crime has 'gone up' (The Guardian, 2016). Anushka Asthana who conducted the above interviews is of Asian origin. Asthana reflected on Britain's past and stated that:

*In the 80s we were the Pakis's, we were the other, we were the ones that we're taking all the school places... and causing the problem and now we just heard it there it's the eastern Europeans and its exactly the same language about a different group... It just shows you how angry and how insecure people are feeling (Asthana, 2016, cited in The Guardian, 2016).*

This ontological return to past was in part spurred on by divisive rhetoric from vote leave. In other examples, the divisive propaganda bequeathed from UKIP's former leader Nigel Farage compelled the former chair of the Conservative Party, Sayeeda Warsi to withdraw support for the leave campaign over claims of hate and xenophobia being peddled (see figure 1).



Figure 1 BBC, 2016[a]

With sections of the public focus on the superficial cause of issues rather than assessing the political and economic system itself, the political dialogue in the UK during the time of Brexit was seldom based on the structural issues that Britain had faced concerning neoliberalism, decades before Eastern Europeans had begun to increasingly arrive in 21st century Britain. Blaming immigrants for the problems that white England faced did not help to inform voters about how difficult it may actually be to leave the EU. Moreover, bracketing out the reality of how difficult and complex delivering Brexit may have resulted in some voters failing to understand the multitudes of issues at hand.

To some extent, some voters were not particularly concerned or interested in how the EU worked before and after the referendum was announced by Prime Minister David Cameron back in 2016 (Google, 2016, cited in Fung, 2016). The latter option would not have surprised Lippmann as he suggested that citizens that find themselves bamboozled by the intricacies of governments and would rather find some form of entertainment in order to peacefully live in 'ignorance' (Lippmann, 1993, p.33-34). In light of this particular viewpoint, after the Brexit vote was decided in favour of leaving the EU, Google announced that searches for "what happens if we leave the EU" had more than tripled (Google, 2016, cited in Fung, 2016).

Albeit Google's revelation is not indicative of wholesale ignorance across the UK, it is quite concerning that this occurred immediately after the announcement of pro-leave victory as opposed to months before the vote which would have informed voters slightly better. In the event that some UK citizens and state figures 'misunderstand' the various issues such as the customs union, the competency of British voters may be brought into question (Google, 2016, cited in Fung, 2016; Rogers, 2019, cited in Stone, 2019). To an extent, Lippmann's bleak assessment of the omniscient citizen being a false ideal bares some relevance and truth in modern society. I do not concur with Lippmann's damning assessment which suggests that citizens are essentially cognitively insipid and incapable of lucid thought.

Nonetheless, in light of propaganda's survival and growth throughout the 20<sup>th</sup> century and into the 21<sup>st</sup> century, assessing the capacity of citizens to interpret propaganda is of great use to academia and society itself. Propaganda is partly welcomed by society and plays a crucial role in helping to reify people's national and social identity and resolving political issues. Rather than expel propaganda, society to some extent has become permeated not only by propagandists and willing propagandees but by the mechanism to spread false information online to millions of citizens. This disturbing projection in conjunction with the possibility that some citizens are not omniscient and increasingly vulnerable to propaganda, re-introducing Lippmann's concept of the phantom public is of great importance to understanding the current threats to democracy.

I have chosen to use Lippmann's conception of the phantom public in this thesis to assess the impact and veracity of modern propaganda attempts. Juxtaposing the assessments of figures from nearly a century ago may appear to be unearthing what has long been buried in the annals of history. Conversely, the issue of citizen's perception being warped by non-state groups, institutions and governments has not disappeared. In fact, to some extent, the issue of perception and propaganda has expanded, due to the use of Internet platforms to spread false information. Therefore, it is hardly a misstep in logic to assume that researchers should attempt to understand the effectiveness of modern propaganda attempts at warping perception.



Considering that the phantom public as a concept underlines issues of perception and apathy towards the political process from citizens and the need for a political class to control and shape citizens, Lippmann's assessments are of value. At this stage, it is necessary to briefly dissect some of Lippmann's hallmark claims from his book *The Phantom Public*, from the early 20<sup>th</sup> century, to demonstrate the necessity of reviving his concepts and descriptions of citizens (Lippmann, 1993, p.33-34). Lippmann took the stance that citizens are irrational and apathetic towards the workings of government and incapable of computing the vastness of information that goes into constructing domestic and foreign affairs. In fact, Lippmann suggested that:

*For the man does not live who can read all the reports that drift across his doorstep or all the dispatches in his newspaper. And if by some development of the radio every man could see and hear all that was happening everywhere, if publicity, in other words, became absolute, how much time could or would he spend watching the Sinking Fund Commission and the Geological Survey? He would probably tune in on the Prince of Wales, or in his desperation, throw off the switch and seek peace in ignorance (Lippmann, 1993, p.33-34).*

Citizens and public opinion, in general, can thus be perceived as an 'irrational force' therefore, inexorably predisposed to making a mess of society should they try to meaningfully participate in democracy (Lippmann, 1993, p.58-59). In order to protect democracy, Lippmann felt it was necessary that "the public must be put in its place, so that it may exercise its powers, but no less and perhaps even more, so that each of us may live free of the trampling and the roar of a bewildered herd" (Lippmann, 1993, p.145). Lippmann viewed society's role as merely voting politicians into power to rule over them. Propaganda was a means to run and control a democracy without resorting to violence in the manner that a despot would (Chomsky, 2002, p.20-21). Public opinion in the view of Lippmann was dangerous and required controlling by a specialised class of people. Accordingly, the public:

*Does not know in most crises what specifically is the truth or the justice of the case, and men are not agreed on what is beautiful and good. Nor does the public rouse itself normally at the existence of evil. It is aroused at evil made manifest*

*by the interruption of a habitual process of life... For did justice, truth, goodness and beauty depend on the spasmodic and crude interventions of public opinion there would be little hope for them in the world. Thus we strip public opinion of any implied duty to deal with the substance of a problem, to make technical decisions, to attempt justice or impose a moral precept. And instead we say that the ideal of public opinion is to align men during the crisis of a problem in such a way as to favour the action of those individuals who may be able to compose the crisis. The power to discern those individuals is the end of the effort to educate public opinion (Lippmann, 1993, p. 57-58).*

From this perspective, citizens appear to be irrelevant to democracy up until a leader needs to be voted into power. Propaganda is the pivotal tool that directs the ‘bewildered herd’ to the necessary ballot choice. Slogans, symbols, incendiary dehumanising remarks and the obfuscation of a balanced argument are paraphernalia to triggering resentment towards out-group leaders and admiration for in-group political candidates. This was present during President Trump’s attacks on Congresswoman Omar, Congresswoman Alexandria Ocasio-Cortez, and Congresswoman Rashida Tlaib in which he told them to ‘go back’ to their countries for criticising America (Trump, 2019).

Days after President Trump made this scathing attack on Twitter he held a rally in Greenville North Carolina to which he began another scathing attack on Congresswoman Omar only to be interrupted by chants of ‘send her back’ (CBS News, 2019; Smith, 2019; Ruiz, 2019). It is worth noting that Congresswoman Omar is a naturalised American citizen who became a US citizen through the same process as the current First Lady Melanie Trump (Smith, 2019; Ruiz, 2019). Furthermore, Congresswoman Alexandria Ocasio-Cortez was born in New York; Congresswoman Rashida Tlaib was born in Michigan (Smith, 2019). This unfortunate example demonstrates Lippmann’s bleak depiction of a society that is irrational and partially unable to rouse itself against evil.

However, it is vital to note that this is a limited case of a phantom-like public as Congresswoman Omar was greeted and welcomed at an airport by her constituents in a sign of solidarity with Congresswoman Omar and the rejection of President Trump’s divisive rhetoric. The crucial point to take from both examples of Brexit and Donald

Trump's incitement of social division is that propaganda has its place in society. Until propaganda is greatly curtailed, it is not an outlandish idea to assess the veracity of concepts that may help to shed light on why propaganda is so welcomed, irrespective of how old the theory may be.

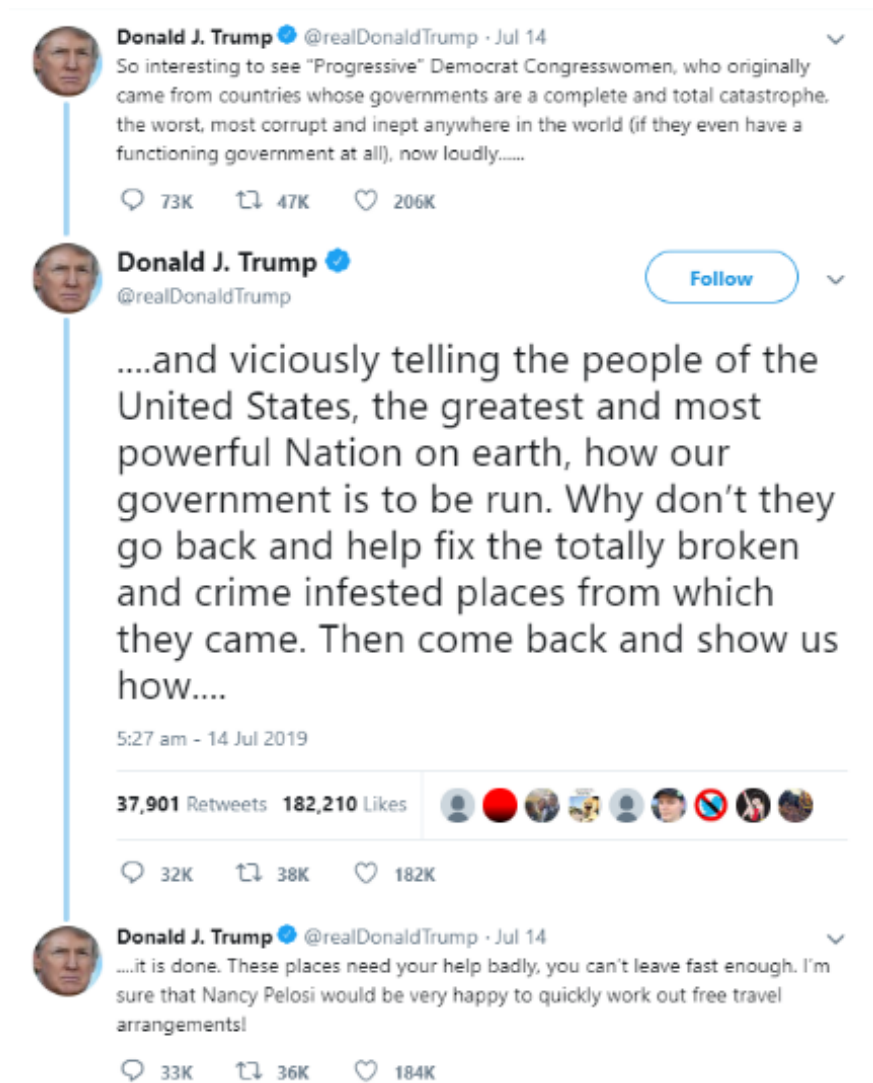


Figure 2: Trump, 2019

Conversely, information on the Internet has provided citizens with the option of attaining knowledge concerning domestic and foreign affairs. Millions of people visit various Internet sites to find information in order to self educate; therefore, some of Lippmann's claims concerning the unflatteringly low appetite of citizens to engage in a democracy is questionable. Nonetheless, the issue of rationality and being able to compute vast swaths of knowledge while having a normal life is still unresolved. When looking at the current landscape of cyberspace, fact-checkers are at times engulfed by the torrent of propaganda that is spread online.

At this stage, it is necessary to ask the pressing question. Is it too soon to assume that the average citizen has learnt from the annals of history on how dangerous it is to fall prey to propaganda that spurs hatred, diplomatic disputes, acts of sanguinary and irrational thinking? Are citizens rational beings that can resist the seductive allure of propaganda and seek out the truth concerning domestic and foreign affairs? The implications of these questions are dark and incredibly condescending. Nonetheless, if irrationality is a permanent feature of society, when it comes to perceiving propaganda, surely assessing whether modern citizens can withstand contemporary blitzkriegs of propaganda is admissible.

To briefly answer these questions, JTRIG did not take the view that citizens are long past fooling. In fact, group psychology, sociology and anthropological insights were vital in aiding GCHQ's new generation of covert online propagandists. Furthermore, according to a JTRIG Slide presentation that was titled *The Art of Deception: Training for a New Generation of Online Covert Operations*, 'People make decisions as parts of groups. People make decisions for emotional reason not rational ones' (The Intercept, 2014). Although GCHQ stopped short of referring to citizens as a phantom, one thing that is clear from this presentation is that decades after Lippmann published the book *The Phantom public*, British spies still view citizens as emotionally vulnerable and susceptible to propaganda (see figure 3). The phantom public is still a relevant theme to study.

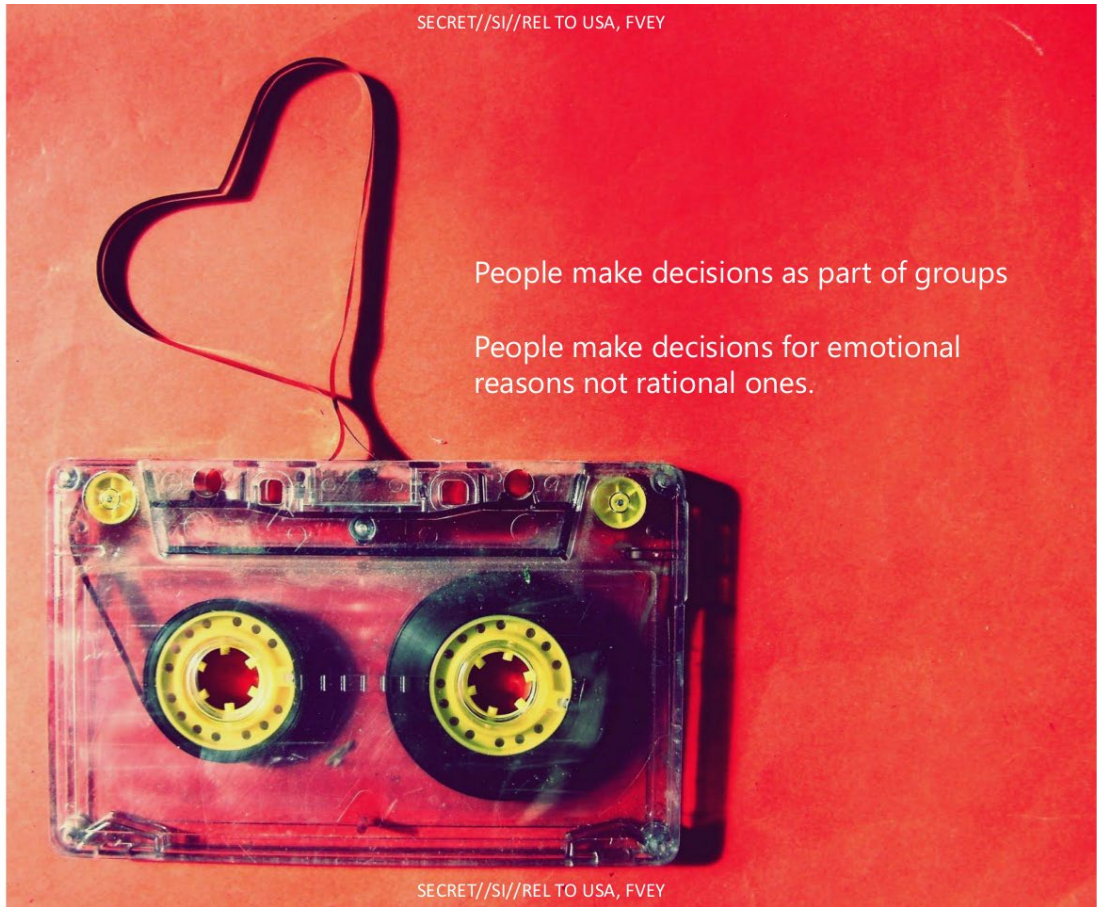


Figure 3: The Intercept, 2014

---

## 1.9 In What Ways is the Modern Public Irrational and Susceptible to Propaganda?

---

Propaganda usually plays to the irrational, reactionary faculty of humankind (Ellul, 1973, p.158). However, at first sight, such a pejorative statement may appear to be an overreach and highly inflammatory. Research from the field of Social Psychology has provided significant insight into how humans package information that can lead to circuited cognitive shortcuts which manifest as vacuous and irrational stereotypes (Haslam, Rothschild, and Ernst, 2002, p.88; Hinton, 2000, p. 22; Pennington, Gillen and Hill, 1999, p.113). This is not to say that all human decisions and judgments are egregiously irrational. However, propagandists seek to capitalise on human emotions, impulses, and incomplete pictures of the world that hampers the ability of individuals and groups to make the most logical decision during elections and evaluate domestic and foreign affairs. When people attempt to interact with the world, packages of cognitive pre-stored information help to identify, provide context and rationalise what it is the individual is experiencing (Pennington, Gillen and Hill, 1999, p.113).

These packages are called schemas (Pennington, Gillen and Hill, 1999, p.113). Schemas are developed from birth throughout childhood and continue into adulthood. Understanding, social cues, hierarchies in society and other social customs can be facilitated through layers of structured knowledge. To be precise, a schema can be used to help people understand social and hierarchical customs. A role schema refers to the 'knowledge structures people have about norms and expected behaviours of people who hold specific role positions in society' (Pennington, Gillen and Hill, 1999, p.113). Schemas effectively help to speed up the categorisation and identification of what it is an individual must contend with. A category can have a litany of descriptive features, i.e. an object that has multiple pages, a front cover with images and writing, a back cover with a blurb, a bar code and price would likely be categorised as a book.

Schematic knowledge is not regulated by an objective arbiter; they are the product of subjective sense-making that has developed from birth. As a consequence, social categorisations may be inaccurate and based on irrational assumptions that are

detrimental to social relations. Social categorisations concerning individuals or groups of people that are markedly different than any given perceiver often produce a list of stereotypes that allows the individual to make sense about his or her experience or perception of others or even in-group people of similar identity. To a great extent, stereotypes can be viewed as a feature of day to day cognitive processes in conjunction with organising and retrieving information in memory (Hinton, 2000, p. 22).

Stereotypes are often a truncated representation of reality in which the perceiver has reduced an individual or group to a handful of assumptions that are usually negative in order to reduce the cognitive load of having to discern the truth from multiple sources. For this reason, it can be said that propaganda ‘appeases...tensions and resolves ...conflicts. It offers facile, ready-made justifications, which are transmitted by society and easily believed’ (Ellul, 1973, p.158). Judging from Ellul’s assessment, indeed, propaganda helps to crystallise and reify internal images and packages of information to explain the world to a group of people in society.

In the view of candidate Trump (back in 2015), Mexicans are rapist and criminals, therefore unworthy of being let into the US despite not being able to verify if they have sexually coerced people or engaged in criminal activity (Trump, 2015 cited in Lee, 2015). In the words of candidate Trump ““What can be simpler or more accurately stated? The Mexican government is forcing their most unwanted people into the United States. They are, in many cases, criminals, drug dealers, rapists, etc”” (Trump, 2015, cited in Lee, 2015).

Stereotypes impute a fixed ‘homogenised image’ and characteristics that operate as a potent form of ‘social control’ which candidate Trump was attempting to wield amidst his followers in relation to Mexico and the issue of border security (Pickering, 2001, p.5). In some instances, propaganda serves to reinforce racial power balances by apotheosising racist tropes which are based on a list of characteristics that are often antithetical with reality. African American runaway slaves that were caught were diagnosed with a mental illness called Drapetomania. Runaway slaves were diagnosed with this term due to the irrational perception that African Americans were bound by nature to serve the white

race. Running away from an ordained duty puzzled white slave owners, which led to the new categorisation of behaviour. For example, in the view of Dr Samuel Cartwright:

*If the white man attempts to oppose the Deity's will, by trying to make the negro anything else than "the submissive knee-bender," (which the Almighty declared he should be,) by trying to raise him to a level with himself, or by putting himself on an equality with the negro; or if he abuses the power which God has given him over his fellow-man, by being cruel to him, or punishing him in anger, or by neglecting to protect him from the wanton abuses of his fellow-servants and all others, or by denying him the usual comforts and necessaries of life, the negro will run away; but if he keeps him in the position that we learn from the Scriptures he was intended to occupy, that is, the position of submission; and if his master or overseer be kind and gracious in his hearing towards him, without condescension, and at the same time ministers to his physical wants, and protects him from abuses, the negro is spell-bound, and cannot run away (PBS, n.d.).*

Dr Cartwright embraced an essentialist representation of African Americans, which inaccurately presupposes that biological essences are immutable and fixed while ‘obscuring the ways in which they are historically and culturally variable, ambiguous and changeable’ (Haslam, Rothschild, and Ernst, 2002, p.88).

Accordingly, essentialist beliefs assume that ‘membership in a category is fixed or immutable, that one cannot readily shed or alter the identity that it bestows. It involves the imputation of an inherent nature, something underlying the surface characteristics of category members’ (Haslam, Rothschild, and Ernst, 2002, p.88). Moreover, it could be argued that human beings often do not factor in multiple extraneous variables and circumstances before making decisions that may affect public affairs. Without factoring in enough variables into an equation, the results or world view may not be sufficient to deal with the problem at hand. Effectively, a short term solution based on a propagandised incomplete picture of reality may only serve the purposes of a propagandist but not of the person who is enraged by the problem he or she is engulfed by.

Propagandists are usually aware of weak fracture points in interpersonal relationships and society in general. Sensationalising current affairs usually leads to societal concerns about



citizens forming opinions based on stereotypes. For example, the knife crime epidemic in London and the UK has been heavily associated with young black males. Rapper and activist Akala was interviewed on Chanel 4 news about this topic and presented a clear statistical analysis on the issue of knives. Accordingly, Akala stated that:

*Every generation pretends gang crime is a new problem so when you look at the press reports they cite in their scholarship it's the same sort of sense of... panic when actually we've had violent youth gangs for 150-200 years maybe even longer... Let's just look at the maths, there are 1.2 million black people in London, in a bad year, 50 of them will kill someone. That's less than 0.004% of the black population. Therefore, anyone that thinks that blackness is a sufficient common denominator for violent crime clearly doesn't understand what a common denominator is (Akala, 2014 cited in Channel 4 News, 2019).*

When factoring in other incidents, reality and perspective of any given topic tend to shift. However, without the interjection of multiple facts, it is easy for society to cast judgments based on irrational beliefs that knife crime is a black issue as opposed to looking at white violent gang culture in Liverpool and Glasgow in the past century (Akala, 2014 cited in Channel 4 News, 2019). Stereotypes act as a shortcut to help explain the world in a simple way without placing cognitive strains or a form of dissonance when an individual has to compute and juggle multiple theories and variables. Accepting truncated packages of knowledge rather than pondering broad, eclectic information can be viewed as an irrational habit that is present in humans. Propagandists are aware of this habit and therefore seek to exploit it.

As such propaganda can be defined as 'the process whereby public opinion is formed and controlled by appeal to the irrational side of man's nature in such a way that it is usually favourable to the interests of those directing the propaganda' (Beaglehole, 1928, p.96). In the 21<sup>st</sup> century, propagandist have not deviated from the idea that instincts and emotions are the prime influencers of human behaviour. Nearly 100 years ago Beaglehole asserted that:

*The secret of the power of modern propaganda, that which made it such a potent instrument for good or evil, lay in the fact that it was directed by those who*

*possessed a scientific knowledge and full understanding of the underlying motives, the fundamental instincts, impulses, and emotions, which are the prime movers of all human activity (Beaglehole 1928, p.94).*

The JTRIG preparation for future online covert analysts acknowledged the need to consider emotional needs such as self-actualisation and esteem needs, as crucial points for targeting people online (The Intercept, 2014).

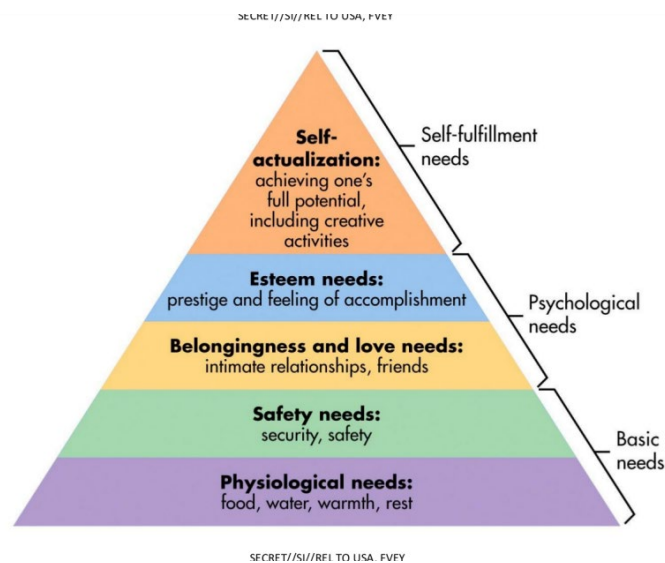


Figure 4: The Intercept, 2014

In doing so, JTRIG is attempting to capitalise on individual and group psychology to produce successful propaganda that can play on people's desires and irrationality. Capitalising on sensationalism and irrationality is not an uncommon practice by propagandists, but in fact, is a point of discussion and focus for GCHQ's modern covert operatives that are entrusted with Britain's global propaganda campaigns.

Propaganda will always find its way to people without much resistance from targets due to the role it plays in helping to explain the world in a simple, digestible manner that confirms irrational social biases. For this reason, it was crucial to analyse the potential of digital propaganda to fool people in modern society in chapter 7. Chapter 7 covers the term tainted leaks, a form of propaganda in which a propagandist has obtained personal and sensitive information about a target, edited this content of information then released it to the world to humiliate and shame the victim. Citizens Lab, a Canadian

interdisciplinary laboratory at the University of Toronto, was able to help investigative journalist David Satter's Tainted Leaks incident by piecing together the modus operandi of the attack. In doing so, Citizens Lab juxtaposed the real and fake documents released to help vindicate Satter.

However, those with preconceived irrational judgments about Satter may fall victim of the tainted leaks campaign directed at Satter. Propaganda thrives among people who are already caught in the gravitational pull of a particular ideology or viewpoint, who refuse to explore other narratives. Moreover, sections of society that are undecided or have very little knowledge of a new incident are also at risk of propaganda. Without a sufficient amount of digital literacy to fact check information, some may not notice propaganda altogether.

Furthermore, amidst the bombardment of *facts* coming from different propagandists online, the individual citizen may not know what to think. As a result, this individual may decide to make a decision based on preconceived notions or, conversely; may choose to avoid siding with any viewpoint, therefore, leaving propaganda with space to exist. The interplay with irrationality, digital literacy and propaganda may shape the future of democratic elections considering the aftermath of the US 2016 presidential election and attempts made to warp perception during the French 2017 presidential elections.

---

## 1.10 State Crime, Human Rights and the Divided Self

---

Sovereign states that enjoy the legal 'monopoly' on the right to exercise coercion to maintain internal stability, at times fall prey to the allure of wielding power excessively (see chapters 3, 4, 5, 6, 7, and 8) (McLaughlin, 2019, p.523). Since the introduction of the UN Charter, the Universal Declaration of Human Rights in 1948 and the subsequent introduction of international courts, protecting citizens has become a fundamental endeavour that has transcended emotional or religious assertions and in many cases is bound to legal maxims. Although it is vital to point out that the Universal Declaration of Human Rights is a not legally binding treaty, its establishment has emphasised human rights standards that have been 'enshrined in other international instruments that are legally binding – such as the International Covenant on Civil and Political Rights'

(OHCHR, 2019[a]). Human rights laws and a general sense of human dignity were not suddenly developed post World War 2 (WW2) but rather, became sanctioned by international law to prevent states from targeting its citizens and the citizens of its adversaries. Although institutions such as the UN pass resolutions that may not be legally binding, states that sign international covenants and agreements, i.e. International Covenant on Civil and Political Rights under the auspices of the UN are ‘effectively binding on States that have ratified them’ (UN, n.d.[a]). In the view of the UN, ‘becoming parties to international treaties States assume obligations and duties under international law to respect, to protect and to fulfil human rights’ (n.d.[a]).

Despite the legal material that has bound states together for the greater good of humankind, nations within the international arena, be it democratic or authoritarian (dictators and autocrats) continue to undermine previous binding covenants concerning human rights and the authority of institutions such as the ICC that enforce human rights law (European Parliament, 2010). For example, states that have signed up to the 1998 Rome Statute of the ICC are supposed to ‘accept the jurisdiction of a permanent international criminal court for the prosecution of the perpetrators of the most serious crimes committed in their territories or by their nationals after the entry into force of the Rome Statute on 1 July 2002’ (ICC, n.d.[a], p.6). Since 2009 the ICC has levelled five arrests warrants against the former dictator of Sudan, Omar Bashir, for ‘60 counts of war crimes and 50 counts of crimes against humanity, such as extermination, murder, rape and torture’ (Bensouda, 2018, cited in UN, 2018[b]).

However, Sudan is not a ‘[s]tate Party to the Rome Statute’ and is not directly subject to the ICC’s jurisdiction (ICC, 2005). Conversely, the UN Security Council referred the case of Darfur to the ICC under resolution 1593 in 2005 (ICC, 2005). Additionally, the ICC has asserted that it may exercise jurisdiction on cases concerning genocide, war crimes and crimes against humanity that have been handed to them by ‘United Nations Security Council... pursuant to a resolution adopted under chapter VII of the UN charter’ (ICC, n.d.[b]). For this reason, the ICC has called for states to arrest Bashir so that he can stand trial (Bensouda, 2018, cited in UN, 2018[b]). Consequently, in 2012 Malawi was due to host the yearly African Union (AU) summit but chose to defer this responsibility because

it did not want Bashir to enter its territory considering the warrant for his arrest (BBC, 2012).

However, back in 2009, the AU voted in favour of ignoring the arrest warrant for Bashir (Amnesty International, 2009[a]; France 24, 2009). Soon after the AU's opposition to the ICC arrest warrant, Kenya, who is a party to the Rome Statute failed to arrest Bashir during his visit to Kenya back in 2010 (European Parliament, 2010). In the immediate aftermath of Bashir's removal from power in 2019, Sudan's military Generals have refused to hand him over to the ICC (Michael, 2019). Judging from the above examples, it is clear that international law and the institutions such as the ICC have been hampered by individual states and regional blocks such as the AU that fail to comply with the ICC, irrespective of whether they have signed the Rome Statute or not. Although crimes against humanity are serious crimes, it appears that states such as Kenya in 2010 were willing to put aside grievances of heinous acts (European Parliament, 2010). When states pick and choose when to help international organisations enforce the law, the respect for international institutions is diminished.

Moreover, war propaganda is prohibited under Article 20 of the International Covenant on Civil and Political Rights, which came into force in 1976 (OHCHR, 2019[a]). However, international law that addresses propaganda is scant and seldom respected by states (The Bureau of Investigative Journalism, 2017; 'United States Of America v. Abdella Ahmad Tounisi', 2013, p.19-25). The US is a party to the International Covenant on Civil and Political Rights but has released war propaganda in Iraq (see chapter 8) (The Bureau of Investigative Journalism, 2017). When states undermine covenants that are legally or illegally binding, other states may potentially choose to mimic disobedient behaviour which chips away at the underlying attempts made to establish international peace. This issue will be addressed in greater detail further into this section. At present, it is vital to briefly address the scope and effectiveness of international agreements that helped to progress the evolution of international law.

International law is not straight forward to grasp in explicit legal terms or even morally. Some have even gone to the extent of denying its existence, considering that some human rights are alien to different cultures and nations (Freeman, 2017, p.6-7). Often, humans

infer meaning on to symbols, notions and phenomena and establish a sense of morality through communication between and within groups (Fulcher and Scott, 2011, p.123). Meaning is, therefore, subject to change over time and between geography. The sociological approach of Symbolic Interactionism suggests that meaning or human understanding is a social product born out of the interaction between people (Blumer, 1969, p.4-7). Our knowledge of the world derives essentially from interpreting and debating stimuli and sensations that bombard our senses.

To a great extent, '[t]he world is never experienced directly but through the ideas that we hold about it. The meaning of reality is, in a fundamental sense, the meaning that we choose to give to it' (Fulcher and Scott, 2011, p. 49). Similarly, the phenomenological approach to explaining the relationship between humans and reality has also emphasised the notion that meaning is socially constructed. Alfred Schultz's phenomenological account of social constructs points to the notion that human constructs are predicated on a biographically determined situation. Definitions that humans create are based on previous experiences and are 'organized in the habitual possessions of his stock of knowledge' (Schultz, 1970, p.73).

Meaning is a result of multiple processes of interpreting and negotiating this assessment within ourselves or with others. Considering the symbiotic and social nature between humans, Schultz suggested that '[o]nly a very small part of my knowledge of the world originates within my personal experience. The greater part is socially derived, handed down to me by my friends, my parents, my teachers and the teachers of my teachers' (Schultz, 1970, p.96). As a consequence of this, questions have been raised about the real objective world and how humans have come to know that objects exist beyond our filtered reality (Spinelli, 2005, p.5).

I do not wish to engage in a Solipsist critique of our ability to verify the objective existence of other humans and objects. Nonetheless, it is crucial to underscore the philosophical tenets that underpin an attempt to explain the vagaries of human perception concerning the construction of meaning, which in the case of human rights, means that this concept (human rights) is not static or universal. In accordance with the pressing issue of reality being fragmented, how are human rights and morality to be expressed

universally? In terms of national security, the responsibility of a sovereign nation to protect its citizens may require exploiting controversial methods of defence such as propaganda and surveillance to fulfil its duty and right to defend its citizens (see chapter 1, 3, 4, 6 and 8). For example, chapter 6 in particular details evidence provided in court which revealed the FBI's online propaganda campaign, that sought to lure terrorist sympathisers to a fake terrorist website that the FBI had created. An email was left at the bottom of the website in the hope that potential targets would email what they thought was terrorist recruiters for the war in Syria but in fact, were FBI operatives. Once individuals began communicating with the FBI, they (FBI) encouraged them to commit acts of terrorism in Syria. American law enforcement uses sting operations as a moral litmus test to see if people are willing to engage in criminal activity.

When US citizens have displayed an interest in criminal behaviour, sting operations are used to test the willingness and readiness of an individual to commit a crime. It would appear that in the presence of war propaganda, the US may have violated Tounisi's human rights that are ensured under article 20 of the International Covenant on Civil and Political Rights (OHCHR, 2019[a]). As a brief reminder article 20 of the International Covenant on Civil and Political Rights clearly states that '[a]ny propaganda for war shall be prohibited by law... Any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law' (OHCHR, 2019[a]).

The issue at hand is that even if a citizen wanted to commit a crime, the FBI has created propaganda to encourage people to join an ongoing war on Syria. In reality, the FBI and therefore the USG have directly espoused war propaganda which goes against article 20 of the International Covenant on Civil and Political Rights, that prohibits any form of propaganda that is used for warfare (OHCHR, 2019[a]). When taking into account that Syria is a sovereign state and a member nation of the UN, it is not farfetched to assume that the US has reneged on its commitment not to produce war propaganda that has incited people to commit crimes against humanity in a foreign nation.

Chapter 6 underscores Tounisi's willingness to engage in Jihad, thus incurring some of the faults. To a degree, the FBI simply stimulated an already would-be terrorist. Setting

up a trap to remove him can be construed as a shrewd act that bolstered US national security and Syrian sovereignty in spite of the fact that the US promulgated war propaganda. Encouraging people to commit acts of terror in another sovereign country is by no means a democratic ideal. If a democratic state is willing to directly or indirectly proselytise an act of terrorism, surely it cannot be said that states have a homogenous liberal sense of self, but rather a duplicitous one that is both liberal and amoral.

At this early point of discussion, it is necessary to ponder the requirement of a state, to balance how it caters to its survival in terms of ensuring sovereignty, protecting its citizens from the threat of hostile foreign actors, domestic criminals and extremists while obeying international covenants concerning human rights. This balancing act is a near-impossible task without infringing upon one or multiple elements of domestic and international law. Threats to a state vary. Subsequently, the vagaries of perception can lead to the misrecognition of the foreign policy of another state due to the importance that one state has to the international system and the adversaries they have (Chernobrov, 2016, p.582). Currently, Iran has far more enemies in the Middle East and the Western world, than Samoa or Norway have.

Consequently, a variety of states must contend with information of impending threats from foreign powers while adhering to human rights concerns. The security apparatus of nations that deals with threats, in many cases encompasses the potential or actual components to commit heinous acts which contravene human rights and a loosely constructed sense of morality. I assert that the state and its ontology or identity are not static, nor is it homogenous. Nations are willing to renege on their ontological narratives of the self that help them construct a particular story about who or what the state claims represent. A so-called democratic state that has convinced itself that freedom and human rights are at the crux of its fundamental DNA and identity can simultaneously engage in acts that go against democratic principles which similar to an authoritarian country. States have a sense of self or ontology that comprises of narratives it produces, historical events and other constructs that help nations to convey a unique identity.

However, in order to deal with the hostile terrain, it must endure, another self, a more amoral self exists at the core of a state foundation. It is incorrect to think of states as



having a national identity or self but rather to see nations as having multiple selves. At times the erratic equilibrium between these selves pushes states into committing criminal acts that violate the sovereignty of other countries or even its domestic laws and sense of self (see chapter 3, 4 and 5). Before discussing these multiple talking points any further with contextual examples, it is vital to define concepts such as the self, human rights and state crime to help illuminate the forthcoming ramifications that such terms will have on the application of propaganda and surveillance campaigns highlighted throughout this thesis.

---

## 1.11 The Self and its Divisions

---

Concepts of a divided self can be traced to Abnormal Psychology (Laing, 1965, p.17-19) in which patients have developed a (pathological) secondary or multiple personalities that in some cases become aware of each other (Cory, 1919, p. 281 - 283). Aside from acute or chronic psychological disorders, the self is a social psychological paradigm that encompasses information concerning self-perception and truncated schematic knowledge about how the world works and how humans are to interact with it. A schema can be defined as a '[cognitive] structure that represents knowledge about a concept or type of stimulus, including its attributes and the relations among those attributes' (Hogg and Vaughan, 2018, p. 51). Essentially a schema is comprised of thoughts, beliefs and attitudes that enable humans to make sense of other objects, people and social circumstances (Hogg and Vaughan, 2018, p. 51).

With regards to the concept of the self, humans cognitively package and store information about perceptions of the self in a similar way to schemas but more intricate and polymorphic (Hogg and Vaughan, 2018, p. 123). Human beings create structures of knowledge that help to formulate a unitary and at times, multifaceted sense of self. These structures of information serve as a map of the world that rationalises an individual's relationship between his or her internal and external reality. The collection of schema-like cognitive constructs about a person's identity or identities can be referred to as the self or selves. Moreover, in the view of Martha et al., the self encompasses 'all the knowledge that a person has about themselves...This includes memories of specific events and experiences, traits, attributes, habits preferences, beliefs, values, plans, hopes

and fears, as well as our knowledge of our social roles and relationship's' (2014, p.187-188).

For the sake of clarity, the self can be defined as a 'set of thoughts and feelings a person has about oneself and... a characteristic way of responding to one's environment... the self is a metaphor for... how a person acts, thinks, and feels toward his or her environment' (Kimble, 1990, p.54). These sets of beliefs that people have can shape their sense of identity, which determines how people think, behave and interpret information. However, how people think, behave and perceive themselves is not always consistent. How an academic chooses to behave in front of his or her students may be completely different from his persona in a staff room or at home with loved ones.

Different selves are used to react to the world that an individual feels is befitting for the situation he or she is in. As such, it may turn out that people have multiple identities and standards that fluctuate in relation to how humans construct the world. If this premise is true 'this would suggest that the commonly held view that the self remains unitary, relatively stable, and 'fixed' over time is an illusion' (Spinelli, 2005, p. 75). Rather, it would make more sense to assume that humans have the capacity for shaping and producing 'different kinds of selves in the same person' (Myers et al., 2010, p.56).

In accordance with Eileen Donahue and colleagues research into the divided self and psychological adjustments, the view was taken that 'the self-concept consists of multiple components or identities... individuals differ systematically in the degree to which their identities are differentiated from each other rather than integrated into a unitary self' (Donahue et al. 1993, p.834). Cognisant of the fact that nations are spearheaded by humans, it is also possible that a country may possess different selves. Locating the self in a state, to an extent is problematic on the basis that the state is fundamentally a composition of institutions and humans. Nonetheless, nations often describe themselves in ways that presuppose the existence of an internal self that is forged by narratives, historical experiences and visions of the future.

As suggested by multiple scholars states possess an ontology or sense of self that can become aggrandised by the circumstances within its immediate and far-reaching

geography (Subotić, 2016, p.610-616; Gustafsson, 2014, p.71-76; Chernobrov, 2016, p.581-586; Kinnvall, and Mitzen, 2017, p.1-6). When nations possess multiple selves, they can make bold claims of being imbued with liberal impulses while simultaneously enabling one or numerous state organs to carry out reprehensible acts on behalf of the state. Due to the fact that perception and morality are essentially socially constructed phenomena's that are dependent on the fluidity of norms, it is possible that two opposing selves can coexist within a state. For example, civil and human rights leader Malcolm X pointed out the hypocritical stance that white America took with regards to the right of African Americans to defend themselves against a saturated culture of lynchings, rape and assassinations. To Malcolm X, liberty and self-determination were applied differently between black and white people and US foreign adversaries:

*You bleed when the white man says bleed; you bite when the white man says bite[,] and you bark when the white man says bark. I hate to say this about us, but it's true. How are you going to be nonviolent in Mississippi, as violent as you were in Korea? How can you justify being nonviolent in Mississippi and Alabama, when your churches are being bombed, and your little girls are being murdered [?] ... If violence is wrong in America, violence is wrong abroad. If it's wrong to be violent defending black women and black children and black babies and black men, then it's wrong for America to draft us and make us violent abroad in [defence] of her. And if it is right for America to draft us, and teach us how to be violent in [defence] of her, then it is right for you and me to do whatever is necessary to defend our own people right here in this country (Malcolm X, 1963, cited in Teaching American History, 2019[a]).*

In this example, the morality of violence is presented as polymorphic dependent on where it is being used and who is engaging in violence. The legacy of slavery and Jim crow infected parts of America with the notion that black life was inferior, therefore, worthy of inhumane treatment. On the other hand, America's democratic self permitted it to continue its claim of being a proud democracy rather than a hostile barbaric rogue state. For this reason, Muhammad Ali felt it necessary to point out that American democracy had brutalised him and other African Americans whereas none of America's adversaries

abroad referred to Ali as a *Nigger* nor *lynched* him or robbed him of his nationality (Ali, 1968, cited in Wolfson, 2018).

To a great extent, African Americans did not experience the ‘American dream but only experienced the American nightmare’ which was a result of the USG harbouring different selves that permitted human rights violations while claiming to be a democratic nation that was opposed to the ills of the Soviet Union (Malcolm X, 1964, cited in Teaching American History, 2019[b]). Fast forward to the 21<sup>st</sup> century; the US continues to be comprised of different selves that are not beholden to the same concept of morality when grappling with external incidents. The Obama administration tackled the issue of Chinese economic cyber-espionage by publicly highlighting Beijing’s alleged activity.

Back in 2014, the Department of Justice went to the extent of charging ‘Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage’ (US Department of Justice, 2014). In doing so, the US Department of Justice cited scathing assessments of Chinese espionage to bolster their sense of indignation. According to John Carlin, Assistant Attorney General for National Security, “‘Cyber theft is real theft and we will hold state-sponsored cyber thieves accountable as we would any other transnational criminal organization that steals our goods and breaks our laws’” (Carlin, 2014, cited in US Department of Justice, 2014).

Similarly, in the view of David Hickton, the US Attorney for the Western District of Pennsylvania, the prosecution of Chinese military hackers ‘vindicates hard working men and women in Western Pennsylvania and around the world who play by the rules and deserve a fair shot’ (Hickton, 2014, cited in US Department of Justice, 2014). While criticising China for its aggressive approach in cyberspace, the US Department of Justice, Hickton, Carlin and the Obama administration failed to inform world leaders that US spies engaged in economic espionage at the detriment of other nations (The Courage Foundation, 2014[a]).

Thanks to Edward Snowden, telecommunications firm Huawei realised that the NSA’s *Shotgiant* program had infiltrated Huawei’s network back in 2010. Leaked NSA slides have revealed that the agency assessed that ‘the increasing role of international companies

and foreign individuals in US information technology supply chains and services will increase the potential for persistent, stealthy' network penetration (The Courage Foundation, 2014[a]).

Considering the fact that millions of citizens around the world use Huawei's products, the right to digital privacy would be violated in China and ironically, in the US. At first sight, some may rightly describe this as an example of Realpolitik. Realpolitik refers to 'a form of politics or diplomacy that is guided by practical considerations, rather than by ideals, morals or principles (Heywood, 2011, p.254). Taking this definition into consideration, if China failed to realise that the US has a sincere democratic and liberal self that is accompanied by a destructive, amoral self which plays a part in shaping foreign policy, China might have left itself open and susceptible to aggressive US cyber operations. Although America is by far, a more democratic state than China in terms of its political structure and prescribed freedoms for citizens; both states appear to be locked in the battle for cyber hegemony (Levite and Jinghua, 2019).

Regardless of the ideological orientation that America claims to have, the US is willing to engage in the very same amoral activity as an authoritarian state that is ideologically on the other side of the political spectrum. This does not mean that America is now an authoritarian regime; rather, the US encompasses elements of malevolence because it (the US) embodies a self that is not rooted in Liberalism. Democratic institutions attempt to manage and regulate this self, but to no avail due to the need for intelligence services to engage hostile environments.

---

## 1.12 State Crime

---

Crimes committed by the state plays a significant part in the destabilisation of the international arena and the degradation of fundamental human rights. State crime essentially refers to 'crimes involving the State acting against its citizens, or against the citizens of another state as part of inter-state conflict, therefore a state is not limited to committing crimes within its own territory' (White, 2008, p. 36). Similarly, state crimes can be defined with an emphasis on domestic and foreign policy, thus bringing focus to the conscious element of international law. As pointed out by Eugene McLaughlin, state

‘crime covers forms of criminality that are committed by nation-states and governments in order to further a variety of domestic and foreign policy’ (2019, p.522-523). However, it is vital to point out that the conscious element of state crime does not mean that all organs of the government are aware of or involved in criminal activity. On the assumption that ‘individuals (e.g. policemen, soldiers, court officials, local administrators) can be regarded as ‘organs of the state’ it would be wrong or at least questionable to assume that the courts are responsible entirely or remotely for extreme crimes committed by another government organ (Dixon, 2013, p.259).

Crimes committed by the state may also be a part of an unofficial or covert campaign as opposed to blatant activity such as Hitler’s use of violence to murder Jews throughout Europe. For example, In 2003 the CIA abducted Abu Omar a terror suspect of the US, on the streets of Milan (Italy) with the help of Italian intelligence officials before Omar was flown to Egypt and tortured (American Civil Liberties Union, 2012). Italy’s highest court has sentenced 23 CIA operatives to jail, although those charged did not attend the trial (CNN, 2009). Members of the US and Italian government that may have been unaware of the scandal cannot share blame for one group or state institution that went rogue. In relation to this watershed divide, Penny Green and Tony Ward have rightfully defined state crime as crime ‘that arises out of some plan, whether official or unofficial, by which state officials coordinate their conduct’ (2012, p.720).

This point is vital to underscore, to avoid misattribution of crimes of one particular backchannel rogue operation from those that operate legally through normal means of conducting domestic and foreign policy. In light of the fact that not everybody is *in on the act* of state criminality, the culture or the ‘organized and planned criminality of secrecy’ by a state to cover up its crimes, makes it difficult to keep track of the extent and true nature of crimes committed. Despite this unfortunate reality, the effects of state crime have been felt throughout the world by millions of citizens (Green and Ward, 2012, p.717).

Currently, the Chinese government have forcibly removed over a million Uighur Muslim citizens to detention facilities to indoctrinate citizens that the state deems to be subversive to Chinese ideology and sovereignty. Although the Chinese government claims that these

citizens went to the camps voluntarily, China has violated the right of citizens to practice religion freely (BBC, 2019[b]). This is an egregious crime which is hard to convincingly cover-up. Guatemala's previous *Memory of Silence* Truth Commission Report details the repressive actions taken by the state that 'eliminated entire Mayan rural communities' during its bloody civil war (Human Rights Data Analysis Group, 2016, p. 23-24). Former military dictator General Efraim Rios Montt was subsequently sentenced to 80 years in jail for genocide and crimes against humanity having ramped up a scorched earth policy that predominantly targeted indigenous Mayan communities in Guatemala during 1982 to 1983 (Human Rights Data Analysis Group, 2016, p. 23-24; Webber, 2018). Argentina's internal *Dirty War* and participation in Operation Condor, an international network of South American states that assassinated, disappeared and tortured political rivals as well as tens of thousands of citizens, is a textbook example of states and their various organs committing crimes against humanity (Dinges, 2005, p.1; National Security Archive (US), 2015).

The FBI, CIA, State Department and other US agencies as well as non-state groups such as Amnesty International, kept track of the gruesome human rights abuses that were being carried out by Argentina's Navy, Police Intelligence, 601 Battalion Military Intelligence and the Presidential office of General (President) Jorge Videla (National Security Archive (US), 1976[a], p.3-5). Details of the severity of the domestic security apparatus to commit murder were regularly highlighted by the CIA. According to one intelligence information cable, the CIA noted that individuals within Argentina's security services and specifically the 'Buenos Aires provincial police would be taking a harder line toward the subversives and that until further notice he wanted no prisoners for interrogation, only cadavers' (National Security Archive (US), 1976[b], p.2).

Former US Secretary of State Henry Kissinger extenuated Argentina's gross violations amidst its battle with the Montenero's and civilians. Kissinger informed Argentina's Foreign Minister Admiral Cesar Augusto Guzzetti that military governments must react to the causes of terrorism while getting their point across to the public before society turns on the military dictatorship (Kissinger, 1976, cited in National Security Archive (US), 2004). Accordingly:

*Let me say, as a friend, that I have noticed that military governments are not always the most effective in dealing with these problems... So after a while, many people who don't understand the situation begin to oppose the military and the problem is compounded. The Chileans, for example, have not succeeded in getting across their initial problem and are increasingly isolated. You will have to make an international effort to have your problems understood. Otherwise, you, too, will come under increasing attack. If there are things that have to be done, you should do them quickly. But you must get back quickly to normal procedure* (Kissinger, 1976, cited in National Security Archive (US), 2004).

The spine chilling advice concerning what needs *to be done*, in context of Argentina's slaughter of civilians, in conjunction with Kissinger's critique of Chile's military government highlights the balancing act states must contend with to maintain sovereignty. Kissinger's blunt advice was partially carried out in terms of delivering a swift, brutal blow to the state's targets. However, concealing state crime became difficult due to the regular protests and demands of mothers and grandmothers of those affected by disappearances, known as the Mothers of the Plaza De Mayo, who wanted to know the status of their abducted children and grandchildren (Hernandez, and BBC Mundo, 2012; Thornton, 2000, p. 281- 283).

President Videla handed power to General Robert Viola in 1981. After the collapse of the military government in 1983, President Videla and various officers came under immense scrutiny. In 1985 President Videla was sentenced to jail; however, this was pardoned by President Carlos Saúl Menem in 1990 (Lopez, 2013). Eventually, this pardon was overturned in 2007. President Videla was sentenced to life in prison in 2010 for torture and deaths of 31 prisoners which was met with jubilation throughout Argentina (Lopez, 2013). Conversely, despite the evidence that may be provided in declassified documents or verbal accounts, not all state crimes are punished to the extent that those who were targeted (or their loved ones) are satisfied with the inquiry.

In the aftermath of Bloody Sunday, an incident in Northern Ireland in which 13 people were shot to death and 16 injured by British Soldiers in 1972, the Widgery Report that investigated this incident 'was perceived as a whitewash of British army activities during



this incident' (Ross, 2000, p.13). Albeit it is essential to note that of late, a victim of British paratroopers who was shot in his chest has recently been awarded £350,000 compensation, thus highlighting the recognition of wrongdoing (BBC, 2019[c]). Furthermore, the Saville report has firmly underscored that:

*None of the casualties shot by soldiers of Support Company was armed with a firearm or (with the probable exception of Gerald Donaghey) a bomb of any description. None was posing any threat of causing death or serious injury. In no case was any warning given before soldiers opened fire (Saddique and French, 2010).*

It would be wrong to assume that all states are above the law and impervious from wrongdoing concerning crimes against humanity. Moreover, cybercrime is a relatively new phenomenon that academics have attempted to dissect (Treadwell, 2013, p. 140). Considering that chapter 5 is predicated on Russian GRU operatives that hacked the DNC server, the concept of cybercrime is essential to grasp. In the view of James Treadwell '[i]nternationally, both governmental and non-state actors engage in cyber-crimes. In the most serious forms of cybercrime, state actors and agencies are involved in sophisticated and high-level espionage' (Treadwell, 2013, p. 140). England's Bedfordshire police have defined cybercrime as an "umbrella" term for lots of different types of crimes which either take place online or where technology is a means and/or target for the attack' (Bedfordshire Police, 2019).

States often take advantage of network vulnerabilities that exist to gain access to a device of another foreign intelligence service or the citizens of that nation. In addition, states can operate under the cover of cyberspace to orchestrate offensive cyber-attacks around the world. This makes it easier for states to engage in a policy of denial regardless of any in-depth conclusions reached by cybersecurity vendors and internal state intelligence services. For example, the USIC has blamed Russia's GRU military intelligence for hacking the DNC to interfere in America's 2016 election (ODNI, 2017[b], p.6). Armed with the cover of cyberspace, Russia has denied this accusation.

Publicly highlighting and holding states to account for crimes in cyberspace is a contentious area, predominantly because states tend to deny any involvement in nefarious

activity. Ironically, even nations such as the US that publicly scold states for engaging in cybercrime chose not to punish the government of Ethiopia for targeting and hacking the computer of a US citizen. US district courts accepted that hacking from abroad in some cases is undesirable but out of their legal jurisdiction. Kidane is an Ethiopian democracy activist that moved to the US (Maryland) in the 1990s. Kidane obtained asylum in the United States but continued his work within the Ethiopian diaspora (local community) ‘to increase awareness of corruption and human rights issues in Ethiopia’ (‘Kidane v. The Federal Republic of Ethiopia’, 2017, p.2). Back in 2013, Citizens Lab stumbled across spyware (Finspy) on Kidane’s computer. Finspy is an advanced form of spyware that was discovered on Kidane’s computer (Sabados, 2014). According to Gamma Group, Finspy is:

*[A] field-proven Remote Monitoring Solution that enables Governments to face the current challenges of monitoring Mobile and Security-Aware Targets that regularly change location, use encrypted and anonymous communication channels and reside in foreign countries (WikiLeaks, 2011, p.1)*

After Finspy was installed on his computer, Kidane’s activities were recorded. According to Nate Cardozo, a Senior Staff Attorney on EFF’s civil liberties team, ‘[a] forensic examination of his computer showed that the Ethiopian government was recording Kidane’s Skype calls, as well as monitoring his (and his family’s) web and email usage’ (EFF, 2017[a]). Also, ‘the infection was active from October 2012 through March 2013, and was stopped just days after researchers’ at the Citizens Lab exposed the Ethiopian government for using Finspy to target Kidane (Cardozo, 2017[a]). The EFF took up this case in court for Kidane against the Ethiopian government. From the viewpoint of the EFF, this case boiled down to whether or not US ‘courts have jurisdiction to hear a case brought by an American citizen for wiretapping and invasion of his privacy that occurred in his living room in suburban Maryland’ (Cardozo, 2017[b]).

Interestingly, a decision was handed down in favour of the Ethiopian government. In short, ‘foreign states are immune from suit unless an exception to the Foreign Sovereign Immunities Act (FSIA) applies’ (‘Kidane v. The Federal Republic of Ethiopia’, 2017, p.2). However, the reasons why US district courts ruled in favour of Ethiopia, emphasises the lack of punitive measures that can be taken against a state for engaging in what some

would deem to be criminal behaviour. To begin with, Kidane’s suit attempted to construe blame on Ethiopia based on the Wiretap Act which prohibits “any person [from] intentionally intercept[ing] . . . any wire, oral, or electronic communication [,]” (‘Kidane v. The Federal Republic of Ethiopia’, 2017, p.3). Additionally, Kidane highlighted that ‘Ethiopia committed the Maryland common law tort of intrusion upon seclusion’ (‘Kidane v. The Federal Republic of Ethiopia’, 2017, p.3). As previously alluded to ‘foreign states are immune from suit unless an exception to the Foreign Sovereign Immunities Act (FSIA) applies’ (‘Kidane v. The Federal Republic of Ethiopia’, 2017, p.2). In reference to 1605(a)(5) of the FISA act, the US district court explained that an exception to this is a ‘noncommercial-tort’ which ‘abrogates sovereign immunity’ from an action involving “personal injury or death, or damage to or loss of property, occurring in the United States’ (‘Kidane v. The Federal Republic of Ethiopia’, 2017, p.2; United States Government Publishing Office, 2011).

The geographical location of the act is imperative as previous examples, including bodily harm, were based on where the tort took place. Interestingly, in the case of *Nilo Jerez v. Republic of Cuba*, it was noted that “the entire tort”—including not only the injury but also the act precipitating that injury—must occur in the United States’ (*Nilo Jerez v. Republic of Cuba, et al*’, 2014, p.8). This signifies that the hack would have had to of physically taken place in the US so that the courts could move forward with Kidane’s claim. As highlighted in the case of *Nilo Jerez v. the Republic of Cuba*, Jerez was infected with hepatitis C while still in Cuba. Jerez’s argument revolved around the assertion that the actions taken against him were similar to that of ‘a foreign agent’s delivery into the United States of an anthrax package or a bomb’ (*Nilo Jerez v. Republic of Cuba, et al*’, 2014, p.9).

Ultimately this comparison was thrown out based on the geographical location of where the harm took place. With regards to Kidane, as a consequence of the original hacking location being outside of the US ‘[i]t thus cannot be said that the entire tort occurred in the United States’ (‘Kidane v. The Federal Republic of Ethiopia’, 2017, p.7). The district court concluded that ‘[f]or the foregoing reasons, we affirm the district court’s dismissal of Kidane’s intrusion-upon-seclusion claim for lack of subject matter jurisdiction. Because the same reasoning applies with equal force to Kidane’s Wiretap Act claim, we

affirm the dismissal of that claim as well' ('Kidane v. The Federal Republic of Ethiopia', 2017, p.10).

At this stage, it is vital to ask the obvious question, what is there to stop another nation from performing the same act but on a larger scale? No one was hurt, and it was done from abroad. In an ironic technicality, according to the US, if nations meet the guidelines set, they are free to hack US nationals without US courts being able to rule in favour of the victims. This does not bode well for privacy activists, nor does it help to squeeze cyber risk back into Pandora's Box. Establishing whether or not a state has engaged in criminal activity in cyberspace is difficult due to the various contours of domestic laws and contextual scenarios. It is therefore difficult to accurately apply a holistic sense of digital human rights to privacy and truthful information without raising subjective concerns about the interpretation of the law and human rights in general. At best, it can be claimed that the actions of the Ethiopian government have violated UN resolution 68/167 that makes a case for the establishment of the right to privacy in the digital age (UN, 2014, p.1-3). Resolution 68/167 has affirmed that all the rights that people have offline apply to citizens online as well as reaffirming:

*[T]he right to privacy, according to which no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, and the right to the protection of the law against such interference, as set out in article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights (UN, 2014, p.2).*

Unfortunately, this resolution is not replete of examples that accentuate the need for states to refrain from engaging in direct forms of propaganda that have been defined and explored in Chapter (1, 2, 3, 4). Cognisant of the fact that this thesis claims that propaganda and surveillance go hand in hand, the UN's 2013 resolution on digital privacy does not go far enough. Only one half of this dynamic duo is addressed which in many cases is incapable of restraining excessive state surveillance of its citizens and those of foreign states. Unsurprisingly, Ethiopia will not be the first and last nation to violate a UN resolution that was adopted by the general assembly towards the end of 2013.

---

## 1.13 Human Rights Defined

---

So far, human rights have been mentioned in association with state crime without a definition or historical context being outlined. For hundreds of years, humans have been subjected to discrimination that occurs as a result of state laws that encourage the stigmatisation and stratification of race class, ethnicity and gender. Jim Crow laws that were established in southern parts of the US were designed to segregate African American citizens from their alleged superior white societal counterparts. In other parts of the world such as South Africa, the system of Apartheid was set up to disenfranchise and segregate black citizens from white citizens. Cognisant of the fact that Jim Crow and the system of apartheid were legal as far as domestic laws are concerned, human rights violations were deemed to be the norm in different parts of the world.

Moreover, post WW2, the world became deeply concerned about the wholesale slaughter that was inflicted on Jews and minorities by Nazi Germany. It became imperative to put into law a universal acknowledgement of fundamental human rights to prevent the horrors endured by millions throughout the world. In 1948 states from all over the world signed the UN declaration of Human rights to provide a fundamental legal buffer to protect citizens from rogue states (United Nations, n.d.[b]). This document included 30 freedoms that accentuated the need for states to respect the ‘the right to freedom from torture, the right to free speech and the right to education’ (Amnesty International, 2018).

In addition, the EU has deemed it necessary to create its own Charter of Fundamental Rights of the European Union (2000) so that all members endorse a strict set of laws that are designed to protect citizens across the EU no matter where a citizen may travel to (within the EU) (EUR-Lex, 2012). Moreover, Thomas Fleiner, has defined human rights as ‘the rights of human beings to live according to their nature and with other human beings’ (1999, p.9). The UN, on the other hand, has provided a slightly more robust and in-depth definition of human rights which outlines specific categories or points of differences to make it clear that everyone is entitled to human rights. According to the UN:

*Human rights are rights inherent to all human beings, regardless of race, sex, nationality, ethnicity, language, religion, or any other status. Human rights include the right to life and liberty, freedom from slavery and torture, freedom of opinion and expression, the right to work and education, and many more. Everyone is entitled to these rights, without discrimination (UN, n.d. [b]).*

In addition, human rights have been defined as rights that ‘people are entitled to by virtue of being human’ (Heywood, 2011, p.304). Conversely, to some the very concept of human rights and its legal establishment is bizarre or at least a point of contention, as certain rights are egregiously fundamental to most people without the need to have them spelt out in the law. The act of murder was deemed in most cases to be immoral before the UN began to formulate a collective narrative and legal guarantee of human rights. Put eloquently by Martti Koskenniemi ‘[s]urely we had a right to life even if article 6 of the Covenant on Civil and political rights seem effective only if they can be accepted on faith – whose absence provided the very reason for having recourse to them’ (2011, p.161).

Furthermore, human rights can be perceived as a social construct that is provided depending on time, geography and culture. For example, in 2015 the former Kenyan President Uhuru Kenyatta rebuked (former) President Obama who in a joint public speech emphasised that ‘the state should not discriminate against people based on their sexual orientation’ (Wall Street Journal, 2015). President Kenyatta responded in highlighting that ‘for Kenyans today, the issue of Gay rights is really a non-issue’ (Wall Street Journal, 2015).

Such a bold assertion flies in the face of the UN’s Declaration of Human Rights, in which article 7 states that ‘[a]ll are equal before the law and are entitled without any discrimination to equal protection of the law. All are entitled to equal protection against any discrimination in violation of this Declaration and against any incitement to such discrimination’ (UN, n.d.[c]). If states have not signed up to legally binding conventions, they may choose not to value institutions such as the ICC and flout human rights laws as was the case of Bashir during his 30 year rule in Sudan (ICC, 2005). Some rights have more importance than others that are deemed to be a non-issue in different parts of the world. Cognisant of the fact that states encompass the sovereignty to enforce their own

laws, '[t]he very idea of human rights flies in the face of the sovereign and territorial integrity of states. Sovereignty gives states the right to do as they please within' its own nation; '[n]obody can tell them how to treat their own citizens' (Pevehouse and Goldstein, 2013, p.225). As suggested previously, meaning is inferred by and between humans. Concepts such as human rights may be of convenience to a state but an inconvenience to others who adhere to different cultural norms that are seen to be fundamental to the identity of the state. As a result, homosexuality is banned in dozens of countries throughout Africa.

Sources of human rights ideas and debate have emanated from religions, philosophical commentators and politicians. In the Old Testament, the decree of Moses, thou shall not kill, highlighted the value of human life. Moreover, in the New Testament Jesus Christ gave two commands that would in the view of Christians, essentially replace the Ten Commandments; '[l]ove the Lord your God with all your heart and with all your soul and with all your mind.' This is the first and greatest commandment. The second most important commandment is... '[l]ove your neighbour as you love yourself' (Matthew 22:37-40). The latter command left a legacy of compassion and encouraged humans to show mercy towards each other as opposed to intolerance and violence. Moreover, philosophers have played a crucial role in developing natural law and accentuating the fundamental qualities that all humans possess, which grants every human the right to life and liberty.

For example, in 1859 British Philosopher John Stuart Mill expressed his belief in universal human rights in claiming that it is 'imperative that human beings should be free to form opinions and to express their opinions without reserve' (Mill, 1992, p.54). This viewpoint turned out to be a fundamental element within the UN Declaration of Human Rights and the Charter of Fundamental Rights of the European Union (EUR-Lex, 2012; United Nations, n.d.,[b]). However, during the period that Mill wrote *On Liberty*, many European powers had only recently banned the trading of slaves and gradually began to outlaw slavery. In fact, in 1859, when *On Liberty* was released, Portugal abolished slavery in the previous year (BBC, n.d.). On the topic of slavery, in 1762, Jean Jacques Rousseau's book *The Social Contract* rebuked slavery on the basis of humans being born with fundamental rights.

Rousseau suggested that to alienate, that is, to give or to sell oneself would require sustenance in return. Operating under the logical impression that no one who is sane would sell themselves into bondage without a return, Rousseau suggested that it is absurd for a man to give himself to the mastery of another for nothing (Rousseau, 1968, p.54). Moreover, if a significant amount of people were to engage in this form of absurdity it would be tantamount to conjuring up a ‘nation of lunatics; and right cannot rest on madness’ (Rousseau, 1968, p.54). By explaining the absurdity of slavery, Rousseau sought to underscore his opposition to human subjugation predominantly because rights cannot be impeded by madness nor illogical cognitive ideas.

Aside from this thought experiment, Rousseau argued that slavery was wrong, particularly when children are born into slavery. In this particular scenario, the slave owner has determined the destiny of another human despite the intrinsic element of freedom and rights that all children are born with. Rousseau emphatically expressed this view in stating that ‘[e]ven if each individual could alienate himself, he cannot alienate his children. For they are born men; they are born free; their liberty belongs to them; no one but they themselves has the right to dispose of it’ (1968, p.54). Although slavery persisted long after 1762, philosophers contributed to the production of inclusive universal human rights even if by being a polemicist or an author of a book opposing the plight and terror that millions suffered worldwide.

Furthermore, human rights narratives and the establishment of human rights laws emanate from the political sphere of society. Ironically, rudimental concepts of limiting state power in England were enshrined to the law during a feud between King John and powerful barons (Geoffrey, 2012, p. 3). King John conceded to the barons and signed the Magna Carta into law in 1215. This new law highlighted the limits of a Kings power and set ‘out the laws which the king and everyone else had to follow for the first time’ (Parliament (UK), n.d.).

A key clause from the Magna Carta still exists in contemporary Britain as law. Clause 40 states that “[n]o free man shall be seized, imprisoned, dispossessed, outlawed, exiled or ruined in any way, nor in any way proceeded against, except by the lawful judgement of



his peers and the law of the land’; a fundamental addition which led to the recognition that people cannot be held inappropriately by the state in the UK (Parliament (UK), n.d.). As time progressed, states began to create laws to bring about a basic set of human rights for citizens. After much pressure and centuries of bloodshed, US President Lyndon B Johnson signed the Civil Rights Act in 1964 which ‘prohibited discrimination on the basis of race, colour, religion, sex or national origin, in public places, provided for the integration of schools and other public facilities, and made employment discrimination illegal’ (Bowen, 2015). Conversely, African Americans are still victims of fiendish modern-day lynchings and systemic racism in the US.

---

## 1.14 State Crimes and the Divided Self

---

So far, research and history have shown that the self is not necessarily a static and homogenous construct, rather a polymorphic and fluid notion or way of being. I assert that states much like individuals encompass multiple selves. Nations can harbour multiple ontologies and simultaneously dissociate themselves with amoral traits and incidents such as human rights abuses. Within the International arena, labelling other countries in order to make sense of interstate relations requires states to ascribe meaning to the labels they bestow on to other nations. In many cases, states prescribe pejorative labels to their adversaries in an attempt to distance themselves with state criminality and amoral behaviour while presenting their targets self in a homogenous manner. What many states fail to do when launching verbal attacks on other nations, is to make clear that although they claim to be responsible and peaceful nations, they too encompass another self that is similar if not identical to the very terms being used to criticise other countries.

States may not openly profess to be deceitful and sinister. However, the repeated actions of nations that are associated with amoral behaviour suggests that states can present a peaceful liberal self while also harbouring a more corrosive and dangerous ontology that pushes states into confrontation or violating the rights of its citizens and the citizens of their adversary. For example, in 1964, many years after America had declared itself the democratic leader of the free world, Malcolm X levelled a verbal attack on the USG in stating that ‘[u]ncle Sam is guilty of violating the human rights of 22 million Afro-Americans right down to the year 1964 and still has the audacity or the nerve to stand up

and represent himself as the leader of the free world. Not only is he a crook he's a hypocrite' (Malcolm X, 1964, cited in Teaching American History, 2019[b]).

Remembering the very nature of state criminality is often an abstract phenomenon for politicians when they engage in verbal criticism of their adversaries. The omission of state criminality is indeed a product of hypocrisy. But it is also a byproduct of states managing different selves which helps the state to make sense of its relationship with its past, present and future (constructed) threats to its survival.

Moreover, when regimes fail to meet the standards of liberal democratic states, the US and other's create 'a special category – that of rogue states. In the case of rogue states, internal regime characteristics – a poor human rights record and lack of democratic credentials – are explicitly linked to expectations of aggressive outward behaviour' (Reinold, 2013, p.119-120). States tend to brand and label their adversaries with a quasi-immobile ontology to depict the international arena as a battle between 'good and evil' (Reinold, 2013, p. 120). After September 11, George Bush presented the nature of multiple authoritarian regimes in order to reveal to the world the true ontological self that rogue states are beholden to, which the US must contend with (Bush, 2002).

President Bush suggested that after 9/11, regimes such as North Korea remained quiet (Bush, 2002). In the case of America's self-proclaimed ability to see into the nature of foreign adversaries, President Bush declared that 'we know their true nature. North Korea is a regime arming with missiles and weapons of mass destruction, while starving its citizens' (Bush, 2002). In the case of Iraq, President Bush portrayed a nation that is determined to destroy its people:

*This is a regime that has already used poison gas to murder thousands of its citizens, leaving the bodies of mothers huddled over their dead children. This is a regime that agreed to international inspections then kicked out the inspectors. This is a regime that has something to hide from the civilized world* (Bush, 2002).

Judging from this example, President Bush sought to contrast Iraq with the US and its *civilised* allies that are driven by a liberal ontology. Essentially states perceive adversaries and allies with temporary and at times fixed ontologies. However, the extent of

*liberalness* is dependent on liberal thinking and actions by the state (Castellino, 2009, p. xiv). When deciphering a state's liberal predilection and ontology Joshua Castellino's approach adopts a:

*[P]ragmatic rather than a Utopian or even scientifically precise view of the liberal state – not focused on the achievement of absolute 'liberalness' but rather focusing on the extent to which steps have been taken to orient the state towards liberal values (Castellino, 2009, p. xiv).*

There is no doubting the existence of America's sizable government apparatus that attempts to root out corruption and human rights abuses. Despite this, the USG pressed forward with an illegal invasion of Iraq and Afghanistan. Furthermore, US drones that are being used to assassinate terrorist worldwide have killed civilians in Afghanistan, Iraq, Yemen, Somalia and Pakistan (Amnesty International, 2009[b]). This issue is compounded further by the fact that in some cases, the US violates the sovereignty of other nations by flying military aircraft and drones in their airspace.

According to Ben Emmerson, the UN's special rapporteur on human rights and counterterrorism "[a]s a matter of international law, the U.S. drone campaign in Pakistan is ... being conducted without the consent of the elected representatives of the people, or the legitimate Government of the State" (Charbonneau, 2013). To compound this moral issue even further, in the past President Bush and many members of America's Congress did not believe that the US armed forces should be subject to the ICC. As a result, President Bush's administration passed the American Service Members Protection Act 2002 which authorised the USG (President) 'to use all means necessary and appropriate to bring about the release' of US armed forces who has been apprehended and detained by the ICC (Office of the Legislative Counsel U.S. House of Representatives, 2013, p.8).

Liberal institutions such as the ICC were set up to make the rule of international law applicable to everyone. Preventing the international rule of law is not democratic nor liberal, which highlights the lack of commitment by powerful rogue states to deter institutions from shaming and punishing state crime. This example provides insight into the theme of this subchapter which revolves around the notion that states have selves that are not always morally symmetrical with one another. States are willing to repeatedly

engage in ethically questionable acts because they harbour another self that is beholden to destructive behaviour patterns which are antithetical to a liberal sense of self. The liberal sense of self is typically presented as the only mode a state embodies even when on the verge of engaging in acts of aggression.

This amoral self often acts as an ironic accomplice to the liberal democratic self that has enabled the state to exist as a functioning homogenous entity that is capable of dealing with socially constructed threats. Since the Snowden leaks became public, NGO's such as Big Brother Watch, Privacy International and Liberty have taken the British government to court over the misuse of its (Britain's) surveillance apparatus to capture large swaths of data for long periods and sharing information with foreign nations (Bowcott, 2015; Big Brother Watch and Others v. The United Kingdom, 2018; Liberty 2019).

The judgement handed down by The Investigatory Powers Tribunal in 2015 concluded that:

*The regime governing the soliciting, receiving, storing and transmitting by UK authorities of private communications of individuals located in the UK, which have been obtained by US authorities pursuant to Prism and/or ... Upstream, contravened Articles 8 or 10 ECHR (Bowcott, 2015; Big Brother Watch and Others v. The United Kingdom, 2018).*

Additionally, in 2019 startling revelations about MI5's handling of personal data produced a scathing critique from Adrian Fulford the UK's Investigatory Powers Commissioner. Fulford lambasted MI5 in stating that it needed to be put in 'special measures' until MI5's historical lack of compliance was rectified (BBC, 2019[a]; Bond, D. 2019).

MI5 was aware for three years that it had failed to 'maintain key safeguards, such as the timely destruction of material' and had provided false assurances to senior judges about its standards when applying for bulk surveillance warrants (Liberty 2019). Although organs of the state have safeguards placed around them to prevent the violation of human rights, the blunt reality is that this will not be the last time that an intelligence unit from a Western nation is caught violating the human rights of its citizens. I do not wish to

characterise MI5 or the security services as fundamentally evil and wretched. Nonetheless, Western states such as the UK and the US that are faced with generational domestic and international threats will feel compelled to commit human rights abuses because it is difficult to suppress the impulse of dealing with risks in perceived hostile environments.

As mentioned previously, an amoral self is an accomplice to the democratic self that needs to be protected from impending threats. To simply switch off or destroy a self that is crucial to the survival of democracy is not an option that states will willingly take even if each self are in part or entirely opposed to each other from an ideological and moral perspective. State crime and human rights violations are a permanent feature of democracy as well as authoritarian states. Moreover, when considering the various concepts that have been discussed thus far, some may be wondering if human rights can be applied to propaganda that incites criminality and terroristic activity. Or put another way, do citizens have the right to truthful information from their government and various organs of the state? This is not to be confused with the right to information which concerns the right of people that have been subject to disappearance and torture. To be precise international law on the right to information applies to the:

*[E]ntitlement to seek and obtain information on: the causes leading to the person's victimization; the causes and conditions pertaining to the gross violations of international human rights law and serious violations of international humanitarian law; the progress and results of the investigation* (United Nations Economic and Social Council, 2006, p.11).

In contrast, I am explicitly referring to whether or not states are or at least should be bound by law and morality to tell the truth to their citizens even when carrying out intelligence operations. International laws and norms that govern information, when applied to online platforms, appears to be ambiguous. The UN Human rights Council has recently passed a resolution that condemns blocking access on the Internet. To be precise the UN human rights council '[a]ffirms also the importance of applying a human rights-based approach in providing and in expanding access to Internet and requests all States to make efforts to bridge the many forms of digital divides' (UN, 2016[a], p.3). Several years later UN

experts condemned the act of countries blocking the Internet to suppress the flow of information during a domestic crisis. At the climax of political turmoil and protests in Sudan, the government chose to shut down the Internet to limit communications between protestors and society in general. UN human rights experts such as Aristide Nononsi, Nyaletsossi Voule and David Kaye rebuked this type of move for shutting down the Internet in a joint statement:

*Access to information and communication services is crucial at times of protests. Restricting or blocking access to Internet services not only adversely affects the enjoyment of the rights to freedom of expression, assembly and participation, but it also has severe effects on protesters demands* (Nononsi, Voule and Kaye, 2019, cited in OHCHR, 2019[b]).

In addition to the claims made by the cohort of UN experts is the glaring fact that suppressing the flow of information in many respects is a form of censorship that states rely on to shape the perception of citizens during a crisis. Accordingly, censorship is a form of propaganda which aims to eviscerate alternative sources of information, leaving only the approved ideas available to shape perception (Henderson, 1943, p.83). From one angle, the above resolution represents the UN's desire to see information flow freely and truthfully. The truth of how dire situations are during internal strife is key to how the UN and world powers react if human rights are being violated.

Evidently, the truth is of fundamental importance, but the right to this (the truth) is not written down in plain terms to mandate that a state must tell its citizens the truth on sensitive matters. Until this grey area is resolved, propaganda will continue to be an international issue for citizens, the nation and critical institutions such as the UN. As previously mentioned, article 20 of the International Covenant on Civil and Political Rights is somewhat clear on war propaganda, but this is not always enforced by states.

As a result of confusion and the lack of a coercive power that acts above all states, governments have fluctuating levels of respect for human rights and the extent to which the truth should be associated with human rights. At this point, it is crucial to ask; is deception the right of the state or are citizens by right, entitled not to be deceived by their

government? At first sight, it may seem ludicrous for a liberal democratic state to want to or feel compelled to lie and spread propaganda to its citizens. On the other hand, deception and misleading *facts* are at the very heart of democratic governance. For example, of late Twitter reminded the UK Conservative party about its policies in light of revelations that the Conservatives changed the name on its twitter account from CCHQPress to factcheckUK during a government debate between Prime Minister Johnson and Jeremy Corbyn (Shirbon, 2019). This move was made to suggest that they were an objective fact-checking account.

The Conservative government's twitter account then proceeded to begin *fact-checking* Jeremy Corbin's narratives, with many people assuming that this account was a bipartisan non-state fact-checking company. To answer an important question concerning whether a state or its organs feel they have the right to deceive people, Conservative MP Dominic Raab responded to criticism about the Conservative government's twitter account stating that "I knock on doors every day...[n]o one gives a toss about the social media cut and thrust. What they care about is the substance of the issues, and of course there's a huge amount of scepticism about the claims of all politicians" (Shirbon, 2019).

However, cognisant of the fact that human perception is subjective and incredibly fragmented, it is of no surprise that Conservative MP's speak with such disdain about the truth and deception. When taking into account that truthful information is critical to making the correct decision in any given affair, it would appear that this should be attributed to some form of human rights. Iraq suffered a blitzkrieg of propaganda concerning weapons of mass destruction before enduring a barrage of missiles from the US and UK who were the main culprits of pushing state propaganda. In light of the fact that some governments are regularly involved in some form of propaganda or misinformation, state crime in association with propaganda is a significant issue.

This moral conundrum is a pressing issue when observers take into account that cyberspace allows intelligence services to create multiple fake identities online and begin communicating with potentially millions (see chapter 1). As highlighted in chapter 1 GCHQ have made it clear that they endeavour to warp perception online through the use of online HUMINT and cyber operations in Argentina, Zimbabwe and other nations

(Dhami, 2011, cited in The Intercept, 2015[a], p.8). At first sight, a critic might assume that it would be utopian to assume that the British government ought to be truthful with the citizens of its adversaries. However, if foreign citizens are fair game, what about domestic citizens? Should domestic citizens have the right to truthful information? In the UK, multiple women have been subject to state spies that have started relationships with them and had children. Back in 2014, the Metropolitan Police agreed to pay a woman £425,000 who was unaware that the man (Bob Robinson) she had sexual relations and a child with, was an undercover spy sent to observe animal rights activists (Casciani, 2014).

However, at present, there is not an exact law or government moral compass that creates clear guidelines for undercover operatives that may need to lie and engage in heinous acts in real-time. The former ex-Director General Lord Jonathan Evans attempted to grapple with this issue in a BBC radio interview but subsequently highlighted how difficult it is to provide clear moral guidelines on what spies can and can not do (BBC Radio 4 Today, 2019). During the exchange with interviewer Mishal Husain, the topic of torture and murder was discussed concerning the remit of undercover agents. Husain went on to ask ‘what if they carry out something like a punishment beating or a kneecapping would that be allowed under the rules?’ (BBC Radio 4 Today, 2019). Lord Evans responded in saying that the:

*Rules are very clear in this game ... process in order to safeguard the public... any difficult complicated ... would be subject to very careful scrutiny, legal opinion would be taken on it, and the process is overseen by a judicial commissioner who is independent of the service (BBC Radio 4 Today, 2019).*

Husain immediately stated ‘But I think that’s a maybe isn’t it? Or it’s a yes... that would be possible’; to which Lord Evans suggested:

*It’s not possible for that to happen without [pause] there are no specific rules on exactly which crimes but there is very clear process to ensure that this is only done at a level which is appropriate which maintains security which maintains the rule of law (BBC Radio 4 Today, 2019).*



From the perspective of Evans, morality is not straight forward in real-time, particularly when the rule of law is at stake. Although this example is slightly different from the aforementioned discussion on human rights and the right to truthful information, it serves as a reminder that morality is polymorphic and subject to interpretation. The truth cannot reign supreme or be the greatest factor for operatives when undercover. Subsequently, it would seem that the right to truthful information is a long way away from being viewed as fundamental to British democracy.

Moreover, it is crucial to reinforce the notion that false information or propaganda can warp the perception of citizens and encourage individuals or groups of people to commit acts of criminality. In light of chapter 6, would the presence of untruthful information as a violation of some form of human right mean that the USG has authorized its intelligence services to violate human rights?

Chapter 6 highlights the use of war propaganda that was used by the FBI to encourage a US citizen to go and fight on behalf of a terrorist group in the Syrian conflict. Regardless of whether or not this particular move by the FBI can be deemed as an act of entrapment, it does appear to be propaganda that was used to encourage an individual to fight in a war. Knowledge of this simple point has not resulted in the US being reprimanded for its conduct and subject to legal proceedings.

Furthermore, at present, the USG has not been subjected to the ICJ for its propaganda and surveillance campaign that was assisted by British PR firm Bell Pottinger in Iraq. Reference to the International Covenant on Civil and Political Rights has been made on multiple occasions throughout this thesis, in spite of the fact that it has not had, a significant deterrence on states to end the production of war propaganda towards states or non-state groups.

It would appear that article 20 of the International Covenant on Civil and Political Rights is simply a colourful sticky-note rather than being an article that states take seriously. Clamping down on state propaganda will be a difficult task in the present and future if nations continue to operate in an international arena that is anarchic or devoid of regulation by a coercive institution that operates above all states. Although it is not a

specific aim of this thesis to dissect international law at great scale, perhaps the case studies presented in the latter stages of the thesis will help to highlight areas that international lawyers or critics need to analyse in order to protect people from propaganda. This, of course, is predicated on the assumption that propaganda is perceived as a social irritant rather than a necessary tool or societal shield.

Exploring key themes such as the self, state crime and human rights at this stage is crucial and serves the purpose of setting out key talking points that will be used to analyse chapter 6. Chapter 6 contains the most important case study that challenges the very nature of Western democracies and their intelligence services. Furthermore, in light of the definitions cited above regarding human rights and state crime, it will be insightful to discuss and explore if this is relevant to Western intelligence services that have used propaganda and surveillance methods to encourage their citizens to engage in acts of terrorism abroad (see chapter 6). Can we refer to propaganda as a human rights violation concerning Tounisi and the FBI's targeted campaigns? The ramifications of such an answer will have significant implications for state crime and concepts of the divided self.

---

## **1.15 International Relations Theory and Cyberspace**

---

This thesis attempts to analyse the inevitable sense of OIS that states and citizens feel when cyber propaganda and surveillance campaigns are revealed. Cyberspace is arguably inexorably bound to the Realist school of thought. Cyberspace is subject to anarchy in which states engage in self-help. Self-help refers to the notion that 'all global actors are independent, they must rely on themselves to provide for their security and well-being' (Blanton and Kegley, 2017, p.24). In effect, states understand that there is no coercive force that acts above states to resolve disputes. As a result of no coercive force that can resolve disputes, states have to look out for their national interest and help themselves or put in other words, engage in self-help. Nations are also suspicious of the activity of other foreign intelligence services and are unlikely to engage in meaningful cyber agreements that significantly reduces cyber-attacks over a long period.

However, the statement that cyberspace is inexorably bound to Realism does not necessarily exclude the capacity or ability for another theoretical lens to be applied to this

domain. Alternatively, states and non-state groups engage in liberal practices for the benefit of striving towards security and peace in cyberspace. For example, French President Emmanuel Macron's 'Paris Call for Trust and Security in Cyberspace' initiative was launched back in 2018 to negotiate and attempt to establish international norms and bolster cybersecurity throughout the world (France Diplomatie, 2019). This initiative has been welcomed by '564 official supporters: 67 States, 139 international and civil society organizations, and 358 entities of the private sector' (France Diplomatie, 2019). States do in fact attempt to forge international partnerships with other states and non-state groups. On the other hand, it is essential to note that France's initiative has been rejected by the US, China and Russia.

In addition, the point could be made that cyberspace enables the expression of freedom by those who only a few centuries ago would not be able to spread messages of dissent towards the government let alone communicate with other citizens around the world instantaneously. The Arab Spring was enabled by cyber communications throughout the Arab world. Similarly, social media platforms have allowed concerned citizens to share video-based content of wrongdoings by politicians in order to educate other citizens. In addition, social media platforms such as Twitter and Instagram enabled citizens around the world to circulate video footage of Donald Trump claiming that he can grab women by the 'pussy' because he is famous (NowThis, 2017).

States tend to be mindful of this expressive capacity and therefore remove various means of communication during civil unrest to curtail the liberal expressive aspect of cyberspace. During the 2019 Indian lockdown of the Indian administered Kashmir territory, the Internet was taken down by the Indian government, most likely out of fear of how cyberspace was instrumental in other 21<sup>st</sup> century uprisings such as the Arab Spring (Goel, Singh, and Yasir, 2019). This form of censorship also helps to prevent domestic citizens from being influenced by an act of disobedience that would likely spur additional support for protests against the government. In shaping perception through censorship of cyberspace, the seemingly incessant battle between liberal ambitions of freedom of expression online and state intervention that warps information and network capacities is symptomatic of the anarchic environment that cyberspace has become.

Furthermore, the argument could be made that private companies have obtained hegemonic control or at least a significant grasp on global data and platforms in which data is produced, i.e. smartphones, laptops, websites search engines etc. This stark reality runs parallel with Marxist conceptions of capitalist exploitation of citizens and the Bourgeoisie having great control of markets and the means of production in conjunction with the state as a reliable partner (Rupert, 2010, p.157-158; Viotti and Kauppi, 2010, p.189).

To an extent, the exploitative aspect of Marxism would be focused today on the data that is collected for manipulation without the individual being able to control what is gathered about him or her. Although the concept of the right to be forgotten has progressed, society is still some way away from this concept being sanctioned into law in which data collectors are placed in a significantly weakened position. Of late, the ECJ has ruled that Google does not have to apply the right to be forgotten on a global scale (Court of Justice of the European Union, 2019, p. 1; Kelion, 2019). Rather, Google only has to remove search results in Europe or put by the ECJ:

*The operator of a search engine is not required to carry out a de-referencing on all It is, however, required to carry out that de-referencing on the versions corresponding to all the Member States and to put in place measures discouraging internet users from gaining access, from one of the Member States, to the links in question which appear on versions of that search engine outside the EU (Court of Justice of the European Union, 2019, p. 1).*

This partial victory for privacy advocates still falls short of transferring full control to citizens concerning sensitive information. In the view of Beck, a new digital modernity has arisen due to the harvesting and exploitation of data by organisations such as the NSA and Google who have effectively become the new *digital intelligentsia* or a part of a 'new transnational digital class, using digital cosmopolitization as a power resource for reshaping the world. These epistemological communities of experts challenge both the nation-state and the citizen' (2016, p.147-148). To a great extent, Marxist undercurrents have manifested in the 21<sup>st</sup> century in the form of state and non-state actors that can shape, monitor and control information flows for profit or national security.

Ironically, the Snowden revelations displayed evidence of US spies revelling in joy at how much information is produced by companies such as Apple for the NSA to intercept (see figure 5). Indeed, private companies may have a huge stake in cyberspace but, intelligence services have developed ways to restore the power balance or equilibrium in their favour, which enables states to ironically throw international (cyber) security into disarray to bolster national security (see chapter 1 and 5).



Figure 5, EFF, 2013[b], p.1-3

When taking in to account the multifaceted nature of the debate, it may be questionable to claim that cyberspace is inexorably bound to realism. Moving beyond theory, the multitude of events that have taken place in this current century alone is enough

justification to assert that cyberspace is in a state of anarchy. Chapter 3 sets out how Liberal Kantesian intuitionist efforts to restrict state self-help actions are beginning to manifest in the form of Brad Smith's Digital Geneva Convention conception. Nonetheless, the best efforts from some of the greatest minds in the private sector are unfortunately not enough at present to restrain states that use non-state entities for their gains in cyberspace at the expense of network security for the rest of the world.

This claim will be outlined in chapter 3 concerning the NSA's plans to push encryption standards on to the global regulatory organisations, which the NSA knows how to circumvent. In effect, liberal institutions remain and function as fodder for powerful states. To reiterate, this does not mean that liberal currents do not exist in the current thinking of states, nor does my approach ridicule the achievements that institutions have made in bolstering network security. Rather, I assert that Realist self-help practises of offensive international cyber operations have had an overwhelming, disruptive impact on cybersecurity and public opinion. Cyber propaganda that is secreted by intelligence services online is yet to be regulated effectively despite the International Covenant on Civil and Political Rights that prohibits war propaganda and right to digital privacy (OHCHR, 2019[a]; UN, 2014).

Furthermore, the inability and unwillingness for liberal institutions such as Facebook to regulate propaganda delivered by politicians has plunged cyberspace into a deeper sense of anarchy concerning online propaganda (see chapter 1). The lack of regulation alongside an international deterrent paves the way for realist self-help tactics to be a significant phenomenon in cyberspace; therefore, leaving cyberspace inexorably bound to Realism.

---

## 1.16 Intelligence Services and the Defence of Empire and Spheres of Influence.

---

It is necessary to make a brief distinction concerning the behaviour of states that have had colonial empires and or possess spheres of influence, in comparison to nations who have no extraterritorial control of other countries or possess self-imposed imperium. Firstly it is vital to note that states must engage in some form of social control to make sure that its citizens adhere to certain laws and social norms (Dean, 2007 p.11; McKinlay, Carter and Pezet, 2012, p.3-5; Lasswell, 1972, p.5). Propaganda and surveillance are two tools that provide law enforcement, intelligence services and other government agencies with the means to shape the perception of its citizens and to help detect criminal activity (Brown, 1963, p.85; House of Commons, 2015[d], p.36; Innes, 2003, p.130).

All states concern themselves with domestic intelligence collection to help combat internal threats. Moreover, many nations are also concerned with potential threats that regional or distant governments and non-state groups may pose (Garraway and Smith, 2017; MI5, n.d.[a]; NCSC, 2018[a]; ODNI, 2017[a], p.5; Rose and Dyomkin, 2017). In a globalised world where the destructive policies of one or several nations can cause a chain reaction of harmful events across the globe, understanding the intentions of foreign states has become a necessary objective for intelligence services (NSA, n.d.[a]; Obama White House, 2014). Effectively, all states are involved with intelligence collection; however small or large it may be.

On the other hand, ambitious colonial, post-colonial and hegemonic states that wish to extend geopolitical influence to regional and international areas of contention are prone to engaging in considerable amounts of intelligence operations. Although it is difficult to quantify the following claim, less powerful states who are not attempting to manage regional and global affairs do not engage in an excessive amount of foreign intelligence operations in comparison to regional or global powers such as the UK or US which have been accused of engaging in mass surveillance (Logan, 2017, p.2; Lyon, 2014[b], p.2). Intelligence operations usually comprise of propaganda and surveillance measures that



gather intelligence or endeavour to shape the perception of targets (see chapter 1, 2, 3 and 4).

Post WW2, key government figures such as George Kennan concluded that America's remit for influence was global (Wilson Center, 1948, p.2). Subsequently, the USG required an international response of political warfare tactics, such as psychological warfare, to reach multiple targets around the world in order to manage the affairs of foreign nations (Wilson Center, 1948, p.2-3). Throughout the Cold War, the US frequently used black propaganda to help facilitate a coup in Guatemala, as well as to tarnish anti-US figures throughout Latin America (Agee, 1975, p.121; Blum, 2003, p.173; Cullather, 1997, p.63; National Security Archive (US), 2017; Office of the Historian, 1975). Due to the proximity that Latin America shared with the US, covert intelligence operations played a vital role in preserving US influence in the Western Hemisphere (Wilson Center, 1948, p.2-3).

However, in order to influence the policy of foreign states that are a part of another nations self-perceived sphere of influence, intelligence services need to be aware of the fluctuations in public opinion on a variety of topics, as well as the stance that political figures within a target nation are proselytising. In some instances, the CIA was able to manage relationships with high-level informants which included former Mexican presidents, as a means of cultivating intelligence from Mexico (National Security Archive (US), 2006[a]).

The Litempo project consisted of the CIA's successful attempts at recruiting informants that provided updates on Mexican social and political affairs as well as the 1968 Tlatelolco massacre (National Security Archive (US), 2006[a]). According to the National Security Archive, revelations about the CIA's relationship with high-level informants within the Mexican government was dated between 1956 and 1969 to which, "President Gustavo Díaz Ordaz and future President Luis Echeverría" provided information to the US (National Security Archive (US), 2006[a]).

In other parts of the world, Britain and France have used their intelligence apparatus to assist in managing insurgencies and conflicts with other nations that were contesting the sovereignty of their respective governments or islands (Porch, 1997, p.341-358). For colonial powers such as the UK and France, it became necessary to extend its intelligence apparatus to capture vital pieces of intelligence within their respective empires or regions of interest.

During Britain's gradual retreat from empire, London hoped to replace colonial possessions with commonwealth states that were friendly and responsive to British geopolitical interests (Aldrich, 2011, p.148). After WW2, several British and French colonial possessions began to press for independence which manifested in armed resistance. Open rebellion prompted both nations (France and Britain) to rely upon their intelligence apparatus to help quell and manage insurgencies. During Imperial Japan's occupation of Malaya, Britain made an uneasy partnership with the Malayan Communist Party (MCP) (Aldrich, 2011, p.149). However, after WW2 the militant forces of the MCP led by Ching Peng launched a rebellion against British rule in 1948 (Aldrich, 2011, p.149).

This rebellion came to be known as the Malayan Emergency in which British, Australian, New Zealand and other Commonwealth nations fought to suppress Malayan insurgents that defied British rule (Australian War Memorial, 2020; New Zealand History, n.d.). Britain mobilised its intelligence apparatus to detect, outmanoeuvre and defeat Malayan guerrilla forces in order to establish control of Malaya and steer the nation's future direction. At the start of the emergency, Britain's intelligence unit known as Special Branch struggled to provide effective intelligence that the army could use (Hack, 1999, p.128).

Conversely, RAF Lancaster aircraft that were equipped with SIGINT capabilities were used to track the radio communications of insurgent forces (Aldrich, 2011, p.149). Moreover, British intelligence did not shy away from capitalising on dirty tricks. Undercover agents sabotaged the communications equipment of MCP's insurgent forces which required repair (Aldrich, 2011, p.149). When the radios were repaired, the

workshops that the insurgents used were bribed so that the radios would emit a stronger signal that the British could detect, locate and target with airstrikes (Aldrich, 2011, p.149 - 150). Intelligence operations became a pivotal tool to help fight this colonial struggle that would determine the future course of Malaya's status. This point is partly justified by the British intelligence assessment which stated that contact "between soldiers and terrorists that resulted in a guerrilla death or capture were directly attributable to good intelligence" (Sunderland, 1964, p.5).

Spies from many nations engage in dirty tricks and covert operations. However, the extent to which intelligence operations are depended upon is predicated on the status and ambitions of a state, particularly if nations identify or previously identified themselves as a colonial regional or global powers. Nations that grant themselves such titles are by default highly concerned about the affairs of other countries. Colonial, post-colonial, regional or global powers must use available tools to penetrate the social-political economic and military layers of a target nation or faction to collect information and if need be, manipulate targets whether they be human or important contraptions such as communications equipment. Without this hyperactive feature to intelligence services of ambitious nations, it may become difficult to manage the affairs of other countries in highly contested regions.

In other examples, the wave of Zionist terrorism that inflicted casualties and instability within British Palestine prompted Britain's intelligence apparatus to focus on multiple factions. Zionist terrorist organisations such as Haganah, Irgun and the Stern Gang engaged in civil agitation, bombing and assassination campaigns against the British administration and armed forces in Palestine. Haganah and Irgun halted hostilities during Britain's fight against Nazi Germany (West, 1988, p.48). However, towards the end of WW2, hostilities resumed. The persistent terroristic activity was designed to convince Britain that its mandate and presence in Palestine was untenable (Charters, 2017, p.115-116).

From a strategic perspective, a British withdrawal from Palestine would facilitate the right political climate to press forward with the creation of Israel on Palestinian territory. Irgun

under the leadership of Menachem Begin who later became Prime Minister of Israel was responsible for multiple attacks on police stations, the 1956 bombing of the British Embassy in Rome as well as acts of sabotage against the Anglo-Iraq pipeline in 1945 (Andrew, 2010, p.353; Walton, 2017; West, 1988, p.49). Similarly, in 1946, the Irgun blew up the British Palestine HQ located at the King David Hotel in Jerusalem (Andrew, 2010, p.351). At times assassination attempts made by Zionist extremists proved to be successful. The Stern Gang managed to assassinate Lord Moyne, who was the British Minister of State in the Middle East (Andrew, 2010, p.351).

Consequently, Britain's intelligence apparatus was used to help determine the nature and inner workings of each Zionist terrorist group that was active. B3a was a British intelligence unit that was responsible for dealing with Zionist terrorism in the region although this was supplemented by the Criminal Investigation Department (CID) that dealt with counterinsurgency in Palestine (Andrew, 2010, p.350; Charters, 2017, p.117). According to David Charters, the CID utilised a litany of intelligence-gathering methods such as the "interception of communications (mail, telephone and telegraph), captured documents and equipment, forensic evidence, plain-clothes surveillance, informers and double agents" (2017, p.118-119). Moreover, MI5 capitalised on SIGINT efforts against Zionist targets in the Middle East (Andrew, 2010, p.353).

Britain relied upon intelligence from the Jewish Agency, which was a non-state representation of the Jewish community in Palestine (Wagner, 2014, p.442). Towards the end of WW2, Britain pushed through a policy of halting Jewish immigration into Palestine, which caused the Jewish Agency to shift its allegiance to supporting terrorism (West, 1988, p.50-51). The Jewish Agency's militia arm, Haganah, perused a campaign of agitation against the British in response to unfavourable policies towards the Zionist cause (Wagner, 2014, p.440). At the time MI5 and British intelligence initially failed to detect The Jewish Agency's shift in allegiance to support terrorism. However, as time progressed, MI5 began to target the communications of the Jewish Agency. Consequently, by 1946, the British was in possession of intelligence which pointed to the Jewish Agency's "complicity with terrorism" (Wagner, 2014, p.448).

This situation soon changed course as a result of British pressure that was placed on the Jewish Agency. After Irgun launched a daring raid on a police station in 1946, the British launched Operation BROADSIDE in which 3000 people were taken into custody from the Jewish Agency's offices in Palestine (West, 1988, p.52). Subsequently, British intelligence managed to piece together information about the Irgun and the Stern Gang which encouraged Haganah to publicly distance itself from armed conflict in conjunction with helping the British to compile a list of Irgun members (West, 1988, p.52-53). Overall, British intelligence was forced to spring into action to help grapple with Zionist extremists in one of its many spheres of influence. The more colonial possessions, mandates and spheres of influence that a nation has, the greater the level of intelligence operations which needs to be performed in order to keep abreast with changing events that may pose challenges and opportunities.

Moreover, British intelligence intercepts alerted London to the imminent invasion preparations being made by Argentina to invade the Falklands. In 1833, the British Royal Navy had removed Argentinean forces from the Falklands and established territorial control of the Island (Falklands Island Government, 2012). Centuries later Argentina attempted to recapture what it saw as its territorial possession, i.e. the Falklands. In the build-up to the 1982 Falklands War, Argentina had been covertly preparing its military to capture the Island. Argentina's invasion had taken Britain by surprise in part due to the speed at which the Buenos Aires moved forward with their invasion schedule (Aldrich, 2011, p.389).

Two days before the invasion of the Falklands, GCHQ had intercepted intelligence from an Argentine submarine that was moving a special forces unit into position to support the invasion (Aldrich, 2011, p.389). Although GCHQ's definitive evidence of Argentina's intentions arrived in the hands of Britain's former Prime Minister Margaret Thatcher two days before the invasion, intelligence intercepts played a crucial role in helping London to decide to send its armed forces to recapture the Falklands (Biles, 2012).

On the other hand, the use of intelligence to manage colonial disputes on the battlefield does not always prove to be successful. Towards the end of WW2 imperial Japan's retreat

from western colonial possessions in Asia presented a short-lived victory for nations such as France, as its colonial possessions in French Indo-China (Laos, Vietnam and Cambodia) had been seeking eventual independence (Porch, 1997, p.298). In 1945 Ho Chi Minh declared the Democratic Republic of Vietnam to the world despite Frances opposition (Rydstrom, 2015, p.195; Porch, 1997, p.298). France began military operations in 1946 to reassert control of Vietnam, particularly in the north of the country (Rydstrom, 2015, p.196). As such, France mobilised its intelligence apparatus to help its armed forces to manoeuvre throughout the protracted war of independence (Université du Québec à Montréal, n.d.). The Service de Documentation Extérieure et de Contre-Espionnage (SDECE) was Frances external counter-espionage unit which operated and played a part in Indo-China to help support French armed forces on the ground (LePage, 2010; Ministry of the Armed Forces (France), 2019). SDECE's SIGINT unit, Section 48, had great success at intercepting "60 to 80 % of the Việt Minh's numerous communications, especially thanks to the radio interceptions from China" (Ministry of the Armed Forces (France), 2019).

However, the infamous Vietnamese victory in 1953 at Dien Bien Phu decimated France's military, which eventually pushed Paris to the negotiation table. Chinese strategic support helped Vietnamese forces to outmanoeuvre French troops at a Garrison in Dien Bien Phu, subsequently leaving them (French armed forces) vulnerable to attack. In the view of Douglas Porch, General Henri Navarre complained that French intelligence was only able to provide radio intercepts of Vietminh forces and "information on the volume of Chinese supplies sent over the border into Tonkin" (1997, p.341). However, the intentions of Vietminh forces were not always known (Université du Québec à Montréal, n.d.). As a result, the amassing of Vietminh forces at Tonkin Delta convinced General Henri that the occupation of Dien Bien Phu "carried few risks" (Porch, 1997, p.341).

This lapse of judgement based on incomplete intelligence led to a decisive defeat for France in Vietnam. This example underscores how vital intelligence is to colonial powers that fought to preserve their status and influence in the region. The above suggestion does not imply that small states do not engage in intelligence operations. Rather, the underlying point to acknowledge is that powerful nations (colonial-post-colonial) that wish to

manage and influence the decision making of other countries are far more prone to engaging in international intelligence operations.

Less powerful states that do not have colonial possessions or military and political spheres of influence may still attempt to alter the political posture of other states. Throughout the Cold War, Norway assisted Britain's intelligence collection efforts by frequently intercepting Soviet satellite intelligence data that was tracking the movements of Argentina's fleet before the outbreak of the Falklands War (Aldrich, 2011, p.401). Subsequently, this information was passed on to Britain, which enabled decision-makers in the British government to eventually form a response to the build-up of Argentina's fleet near the Falklands (Aldrich, 2011, p.401).

Effectively, smaller nations that do not aspire or possess the capacity to take up the mantle as a regional power can still engage in intelligence efforts that shape international affairs by engaging in covert intelligence operations. Propaganda and surveillance efforts are virtually universal; used by all states in one form or another regardless of whether a state is a democracy or authoritarian, colonial, post-colonial or a modern global power. Countries such as the UK and the US that have extensive colonial and post-colonial experiences which are continuously attempting to manage the affairs of nations and regions by using propaganda and surveillance methods, do so to protect what they see as their national interest.

Such interventions may appear to contradict the democratic shell that Western states reside behind, but this is the nature of how states (ontologically) attempt to play a balancing act to satisfy different ontologies or selves. Throughout this thesis, I assert that states have different selves which comprise of a set of national tropes, stories and self-perceived affinities to certain noble ideals. Although the tools of intelligence operations, i.e. propaganda and surveillance may be deemed as amoral, depending on how they are used, states, particularly Western states, tend to hide behind their democratic self to extenuate covert activity towards foreign targets.

This does not mean that two or more selves can not coexist simultaneously. Many nations, such as the UK and the US, allow their intelligence services to make occasional public statements, which at times, is welcomed by society. In spite of this, Western countries often present themselves as liberal, democratic, rational and friendly, which appears to contradict the impulses and traits that states have while operating in the shadows. In fact, chapter 3, 6 and 8 highlights some of the similarities between Western and authoritarian states with regards to intelligence operations. The underlying point to acknowledge is that all states use propaganda and surveillance to meet an end goal. Conversely, colonial and post-colonial powers as well as regional and great powers that are attempting to clamour as much influence as possible, are far more prone to engaging in controversial intelligence operations.

Thus far, examples provided concern Cold War flashpoints but do not demonstrate states or global powers in a contemporary setting in order to reinforce the notion that ambitious modern powers with plans of managing international affairs frequently engage in extensive intelligence operations. Since the Cold War, post-colonial states that have global ambitions for detecting and shaping various spheres of influence have persisted with global intelligence operations. For example, GCHQ's data repository named Black Hole stored internet data such as internet browsing history and search engine queries, which had been collected by tapping international fibre optic cables (Gallagher, 2015). Between 2007 and 2009, GCHQ stored an excess of 1.1 trillion 'events' or metadata records that were swept up through its global intelligence endeavours (Gallagher, 2015).

Moreover, in 2009 the US was keen to understand Japan's key talking points on issues concerning the World Trade Organisation, before an Organization for Economic Cooperation and Development (OECD) event in Paris (WikiLeaks, n.d., p.1-2). As a consequence, the NSA began intercepting sensitive Japanese government communications which provided a draft of key talking points that were to be discussed by Japan's representatives at OECD (WikiLeaks, n.d., p.1-2). Similarly, in 2003 the US bragged in internal communications about its capacity to "shepherd a UN Security Council Resolution through the UNSC" as a result of the NSA's aggressive surveillance of foreign targets. The US was concerned about how nations were going to vote on UN



resolution 1511 concerning reconstruction and peacekeeping in Iraq in conjunction with having this resolution passed before a donors conference for Iraq.

In order to prepare US diplomats for potential issues, the NSA was tasked with spying on foreign diplomats. According to a leaked Top Secret document, the NSA's intercepts 'provided a window into the planning and intentions of the principal players on the Council - and may have even provided the Secretary of State and the U.S. Permanent Representative to the UN with the key information needed to ensure the unanimous vote' (The Intercept, 2016, p.1). In light of the two examples above, it is clear to see that the US has the capacity to engage in international surveillance campaigns which has had a material impact on multiple nations.

Although Britain and the US do not possess colonial status in the 21<sup>st</sup> century, their status as global powers drives both nations to persist with extensive intelligence operations. However, regardless of the status of a country, the desire to understand and shape foreign affairs requires intelligence services to operate in the shadows. As alluded to above, the action of a nation during an international crisis can have long-lasting ramifications for other countries who may not be involved. For example, the potential for conflict between the US and Iran poses economic woes for nations around the world in the event that Iran closes the Straits of Hormuz and prevents the transportation of oil and other goods (ZeroHedge, 2019).

Therefore, irrespective of whether a nation has or has not possessed a colonial empire or the status as a regional or global power, it is desirable for countries who may not be directly involved in the spat between Washington and Tehran to gather intelligence in order to prepare for the consequences. This particular scenario came to light in 2019, when Japan, who is not considered to be a regional military power in the Middle East, sent a naval destroyer to the region partly for intelligence gathering purposes, amidst the crisis between Washington and Tehran (Yamaguchi, 2020).

Effectively, it is in the national interest for a vast amount of nations to engage in intelligence operations in order to keep track of potential or current international

flashpoints as a means of managing the social, economic and geopolitical fallout. Conversely, nations that wish to shape global affairs must frequently engage in intelligence operations. For this reason, countries such as the UK and the US that have had colonial possessions in the past but insist on remaining as global powers, have a global HUMINT and SIGINT capabilities.

---

## 1.7 Methodology

---

Qualitative research methods such as Interpretive Phenomenological Analysis Critical Discourse Analysis and Discursive Psychology, are prominent research tools which are used to analyse discourse (Edwards and Potter, 1992, p.11-12; Fairclough, 2010, p.10-11; Reid, Flowers and Larkin, 2005, p.20). In particular, the aim of IPA is ‘to explore in detail how participants are making sense of their personal and social world’ (Smith and Osborn, 2003, p.25). Conversely, quantitative methods such as questionnaires enable researchers to gather large volumes of data that qualitative methodologies would struggle to produce. Albeit a large proportion of researchers opt to produce raw information from quantitative questionnaires or qualitative semi-structured interviews ‘[i]n many cases, researchers do not *produce* data, but instead *use* existing data for the analysis’ (Flick, 2014, p.44).

My research is not based on quantitative or qualitative research that produces raw data in the form of answered questionnaires, or responses from my own conducted semi-structured interviews. A large proportion of information cited in this thesis is based on declassified or leaked documents, which I analysed and juxtaposed with various other sources of information. I have decided to use document analysis and modern Internet-based research as my form of secondary analysis. Document analysis is an alternative qualitative methodology. Researchers that use document analysis ‘can use already *existing* materials, such as documents’ to further their inquiry (Flick, 2015, p.152).

Document analysis is a form of secondary research, meaning that researchers scrutinise information that was not produced by their project but instead used existing datasets (Flick, 2015, p.152). For some time ‘[m]any researchers use data from the available data archives ... for *secondary analysis*’ thus highlighting the feasibility of document analysis (Bailey, 1994, p.299). Secondary analysis is an attractive approach for researchers since information is ‘collected, analysed and archived by public and government authorities’

(Sarantakos, 2013, p.312). As a result, longitudinal comparisons can be made in society and in many cases between different societies around the world (Sarantakos, 2013, p.312). The longitudinal juxtaposition between documents that already exist and current affairs is at the heart of my thesis.

Therefore, secondary analysis is critical to my work. Declassified information concerning British propaganda activity in Nigeria and Latin America was obtained from The National Archives (TNA) in Kew Gardens (London), making my thesis a form of secondary analysis. A litany of declassified files was thoroughly analysed in order to retrieve the most relevant information on British propaganda activity throughout the Cold War. Declassified information on British propaganda in Latin America and Nigeria was not retrieved via digitised records to copy and paste, but solely through reading the physical copy at the TNA and typing the contents into Microsoft Word.

This form of research has advanced my inquiry significantly, as a result of having access to declassified files in the TNA. However, one immediate drawback that may have future repercussions on my research is the fact that many declassified documents in TNA may be challenging to find. For example, in any given file, dozens upon dozens of letters and documents are compiled together. Some pages are numbered whereas some documents did not have page numbers. However, within any given file, documents that are separate from one another have their own separate page numbers as opposed to one continuous page numbering. Therefore, to find a quote from my work, one will have to tirelessly delve into huge files as there is no contents page. This is not an impossible task, but many may find it challenging to track down the exact quote.

When questioning the staff at TNA about this problem, their retort was *you cannot do everything for them; they have to do their hard work as well*. Irrespective of TNA's justification, this issue could prove to be detrimental to the replicability of my work. To try and remedy this issue, I have taken photos of declassified documents and placed them in the appendices. On the other hand, a distinct advantage of secondary research and document analysis is that I do not need to collect data in the same way as other research methods mandate. I have saved a significant amount of time to focus on analysis. Furthermore, document analysis enables academics to traverse time and geography to conduct 'research on subjects to which the researcher does not have physical access, and

thus cannot study by any other method' (Bailey, 1994, p.294). In other words, inaccessible groups of people from intelligence services that are dead, live on through the letters and reports they have authored that have now become documents in an archive. This benefit has allowed me to analyse documents containing information on British and American propaganda from people who may be deceased or socially inaccessible. It is also important to note that this form of research is relatively cheap.

An additional reason I have chosen to use document analysis is due to the systemic issues associated with qualitative semi-structured interviews and quantitative questionnaires. A well-known drawback of quantitative questionnaires or semi-structured interviews is that they are time-consuming. A further issue is that quantitative or qualitative approaches could cause distress, depending on the sensitivity of the topic. Considering that my research is based on existentially sensitive areas such as covert intelligence that infiltrates the private lives of people, focusing on documents allows me to avoid causing direct harm or incurring major ethical concerns. In other words '[a]nother way you can study human behaviour unobtrusively is through written texts in the form of documents and records' (Esterberg, 2002, p.121).

Fortunately, document analysis allows me to study recorded responses to events in solitude without inflicting disturbance or psychological strain on others impacted by the study. I do not have to ask hundreds of people to fill out a questionnaire, nor post any requests to do the former online. In many respects, my research poses less ethical concerns to society or myself. On the other hand, it must be noted that the Snowden leaks inspired this thesis. It is vital to note that Snowden's decision to steal classified information and leak them to the public is illegal. Nonetheless, various researchers have written on this subject area, to expand knowledge within their respective fields (Stoycheff, 2016, p.298; Lyon, 2014[b], p.1; Lyon, 2015, p.139-140; Murphy, 2014, p.194; Van der Velden, 2015, p.182).

However, there are some limitations with regards to document analysis. For example, certain topic areas, e.g. IRD activity in Jamaica, have produced a limited amount of documents. If this is the case because the government has refused to grant public access to these files, researching niche areas such as IRD operations in Jamaica will be an issue. Moreover, when covert intelligence operations fail and become public knowledge,

concerns of government cover-ups make it difficult for academics to conduct research and provide a clear holistic picture of what takes place in the shadows. This was a prominent issue during the Bunter Crabb affair in which a British Intelligence mission against a Russian warship in Portsmouth led to the mysterious death of one of its agents. In a rare visit to the UK 'Soviet leaders Nikita Khrushchev and Nikolai Bulganin' arrived at Portsmouth harbour in 1956 (BBC, 2015[a]). Lionel Crabb 'carried out an intelligence operation against Russian warships in Portsmouth Harbour – a diving mission from which he had not returned' (Bennet, 2016). Analysis from Moran has indicated that '[a]s details of secret service involvement in the operation were unearthed, Her Majesty's Government (HMG) retreated behind a wall of silence, a strategy consistent with the age-old convention to disavow all knowledge of intelligence operations' (2011, p.677).

The former British Prime Minister Anthony Eden went a step further, stating that 'it would not be in the public interest to disclose the circumstances in which Crabb met his death' (Eden, 1956). Albeit this case was during the Cold War, the British government's firm stance on secreting sensitive information has stood the test of time. In response to the release of Top Secret documents by Snowden beginning in 2013, GCHQ stood by their mantra 'we do not comment on intelligence matters' (GCHQ, 2014, cited in Ackerman and Ball, 2014).

Moreover, when trying to access documents created or owned by foreign governments, the issue of language is another hindrance to my research progression and general understanding. Although my research is predominantly based on British and American intelligence services, building up knowledge on the history of foreign intelligence apparatuses could have helped in understanding how other nations view Britain and the US. Furthermore, document analysis only permits researchers to draw deductive conclusions from research as opposed to producing raw data from semi-structured interviews or being in the field as an intelligence analyst. Other methodologies that compel researchers to produce data can enable an observer to look back at original postulations and see whether their results are correct or of any relevance. On the other hand, a significant weakness of my work is that this juxtaposition is not entirely possible.

In many respects, I am in danger of selecting documents or examples that continuously exonerate my discussion points as opposed to producing data that may conflict with my

assumptions. To counter this issue, I have made sure to aggressively evaluate the merits of my research in each case study. Additionally, I have analysed potential weak points or counterpoints throughout this thesis to provide a broader perspective. In doing so, I have explored counterpoints that in some cases, contain elements of truths which contradict assertions made by myself (see chapter 6 and 7).

Also, it is essential to note that documents may have skewed undertones. Put bluntly by Kenneth Bailey; documents may ‘include those events that make the author look good and exclude those that cast him or her in a negative light’ (1994 p.296). Building on this particular point, a researcher is exposed to the risk that ‘original data may contain errors that the secondary researcher is not able to detect’ which in many respects makes my research inexorably bound to a potential amount of flawed assumptions (Bailey, 1994, p.299). However, it is essential to note that this standard applies to interviewees, who could be lying about their answer in a semi-structured interview or a standard quantitative questionnaire. Having said this, Tim May has weighed in on this issue emphasising that:

*History itself and our understanding of it can be informed by a selective reading of documents or those documents themselves may also be selective. Thus, what people decide to record, to leave in or take out, is itself informed by decisions which relate to the social, political and economic environment of which they are a part. History, like all social and natural sciences, is amenable to manipulation and selective influence. In undertaking documentary research, we should be aware of these influences and not assume that documents are simply neutral artefacts from the past (May, 2011, p.215).*

While it is impossible to avoid any form of bias when undertaking document analysis, I have read extensively on multiple areas to search for contradictions. Furthermore, in most cases, ‘documents are easily accessible, replication is possible’ thus enabling my work to be verified by experts in the field (Sarantakos, 2013, p.313). It is also worth noting that of late, intelligence services such as the FBI and the CIA have released a sizable amount of data on their websites, which reveals the anti-democratic and destructive nature of their predecessors. Similarly, the British government have released various documents on the extent of the IRD’s international propaganda campaign. While it can be claimed that

documents have been watered down or altered in some way by the original author, the aforementioned intelligence services have released information that places them in an unfavourable light. Therefore, the claim of bias can only go so far. British and American governments have come some way by releasing information that exposes their double standards on respect for democracy and an international rules-based system.

In terms of the actual research process, I have used several online websites such as The Intercept that are specialised in reporting on leaked material concerning propaganda and surveillance. Although in academia books may be considered as a more appropriate source of information, the 'digital turn' has opened up the academic world to a vast amount of knowledge that resides in cyberspace (Nicholson, 2013, p.63). In the 21<sup>st</sup> century, scholars such as David Berry have accentuated the view that 'it is rare to find an academic today who has had no access to digital technology as part of their research activity' (2011, p.1). Therefore, aside from physical archival research, the majority of declassified research was gathered from online vaults or official websites of various intelligence services. The FBI, NSA, ODNI, CIA, and MI5's websites have been used for my research. Digitised archives have played a fundamental role in acquiring knowledge on foreign intelligence services such as the CIA, NSA and the FBI. Without these organisations digitising intelligence, it may have been challenging to carry out my research.

In the case of the FBI, its online vault of declassified material did not allow me to copy and paste content on to Microsoft Word. As a result of this fact, I had to read and type my findings into Microsoft Word. While this was time-consuming, it provided me with a vast amount of data. It is of great importance to note that a considerable amount of online documents are not uploaded as one whole file that stretches from page 1 to the very end. Often some declassified files contain an assortment of documents that may start from page 1 or in some cases different numbers. To avoid confusion, I have decided to quote page numbers concerning the PDF page number as opposed to the number on the page. This way, all readers can go back and see exactly what page I am referring to.

I have chosen to use this rule for declassified documents, government reports and other research papers. The only exception to this rule was academic journal articles. Additionally, the dates that have been attributed to declassified documents need to be

briefly explained. Initially, I decided it was correct to use the digital release date of declassified documents. In some cases no digital release date is visible. Therefore, if there is no digital release date, but the original date is on the front of the document, e.g. 1956, I have opted to use the date that is actually on the document. If a digital release date is present, e.g. 2016, I have used that particular date.

Conversely, I have salvaged a considerable amount of Top Secret information from leaked sources such as Snowden that were distributed by prominent news outlets such as The Guardian, NBC News and The Intercept. Also, websites such as WikiLeaks was used sparingly to gain a greater understanding of surveillance operations as opposed to being a huge source of information to quote. Nonetheless, data from WikiLeaks was used. Also, mainstream news websites such as the BBC, RT, Al Jazeera and France 24 have been of great use to my research. Although, it is essential to note that I have tried to avoid overusing journalistic sources, in favour of actual declassified or leaked material. Making frequent use of generalised and to some extent, cliché sources such as an *undisclosed source at the White House*, that cannot be verified poses questions of authenticity which I intend to avoid. This is not to indicate that I have ignored a source from American news outlets that cannot be verified in terms of its exact source. Instead, I have tried to avoid whisper campaigns that may be construed as erroneous conjecture.

Provided that leaked physical or digital copies are legitimate, I have made use of them. However, this is a very contentious area. Chapter 8 is primordially based on the words of a disgruntled employee Martin Wells, who left the disgraced firm, Bell Pottinger. Wells later revealed to the world what his job role was in editing propaganda for the US to use in Iraq during the second Gulf War. On a technicality, such claims made may be difficult to state as a fact. Fortunately, what Well's has said in many respects was backed up by Lord Bell, the former chairman of Bell Pottinger. The latter conceded to Wells's claims that the company (Bell Pottinger) reported to the Pentagon, the CIA and the State Department (Fielding-Smith, Black and Ungood-Thomas, 2016).

On the other hand, Chapter 6 is based on an FBI Special Agent (SA) that was compelled to give statements as opposed to him being a fired and resentful former employee. Moreover, I have made use of online information from research institutions. Institutions such as Citizens Lab specialise in investigating complex surveillance and disinformation



campaigns. As a result, I have used a large amount of information from Citizens Lab. Similarly, other groups, such as the Federation of American Scientist's (FAS) and RAND, have been used.

Furthermore, government websites encompass a considerable amount of information concerning surveillance and propaganda activity. UK laws such as the Data Retention Investigatory Powers Act (DRIPA), or the recent 2016 IPA can be found and downloaded on official UK government websites. Also, the British Government has attempted to breakdown sensitive areas of surveillance laws. For example, EI is a contentious area that the British government tried to provide a condensed step by step guide on the nature of EI and bulk EI (House of Commons, 2015[a], p.1; (House of Commons, 2015[b], p.1). These condensed guides were cited in this thesis.

Additionally, other online sources such as YouTube were used to obtain information concerning academics such as Chomsky, institutions such as NATO or news stations such as CNN. YouTube has been useful in tracking previous interviews, particularly those of US Democratic Senators who were at the time responding to the alleged Russian propaganda and surveillance campaigns during the 2016 presidential election. Chapter 5 is based on the comments of Senator Elizabeth Warren, Senator Eric Swalwell and Senator Mark Warner, which was retrieved from interviews uploaded to YouTube. Secondary data from other scholars were used considerably throughout this thesis. Information ascertained from various books at my university library (Middlesex University) played a pivotal role in developing my understanding of propaganda and surveillance.

Furthermore, my literature review was supplemented by information gathered from books that do not exist at Middlesex University. Online Journal articles concerning propaganda, surveillance, democracy and intelligence ethics have been used regularly for the literature review, history section and various other chapters. However, there are certain limitations of employing online research. To begin with, web links for a particular declassified article may cease to exist in the future. Often, websites have a relatively short lifespan in comparison to physical archive or a library. Interested parties may now find themselves in a digital wild goose chase, searching for the original document which could quite literally never be traced. While this is a hypothetical scenario, it is necessary to highlight

the heightened risk of the general public being unable to find a sizable portion of my work.

Additionally, Niels Brügger and Niels Ole Finnemann have rightfully noted the dangers of uploading documents to the Internet which are then open to misuse. According to Brügger and Finnemann ‘archived Web material is an edited, “reborn” version of what was online. However, once data or information has entered the World Wide Web archive, it is also ‘editable’ (2013, p.77). Undoubtedly, this exposes online researchers to the considerable risk of deception that may discredit online scholarship. In general, conducting online digital archival or website based research was beneficial. It is essential to highlight that other ‘[r]esearchers have been quick to grasp the practical benefits’ of digital research, predominantly due to the ‘Improvements in speed, access, volume and convenience are routinely celebrated’ (Nicholson, 2013, p.61). Despite the flaws that exist in conducting digital research, writing this thesis would have been nearly impossible without using online information.

To conclude with words of Janine Solberg, despite the systemic flaws of document and digital research, it can be said that ‘[t]he promise of mass digitization can thus be seen to represent, on the one hand, a widening of access and discovery and new means to recover marginalized or forgotten rhetoric’s and, on the other’ (2012, p.71). As a result, document analysis from predominantly online archives will be used in this thesis.

---

## **1.8 Structure of the Thesis**

---

Considering that this thesis has brought together the two fields of propaganda and surveillance in conjunction with OIS, Realism and various other theoretical or conceptual postulations, it was necessary to divide this thesis systematically. To set the scene for why my thesis is necessary, I undertook the task of highlighting fundamental intelligence issues that the world currently faces. Chapter 1 introduces both propaganda and surveillance, along with the current issues that have caused OIS for states and their citizens. Also, Chapter 1 highlights the aims and purpose of this thesis. After the scene is set, it was vital to introduce the methodology, albeit still within the same chapter (chapter 1). The advantage of doing this is to clear up any possible confusion that could occur

regarding how I am going to research three contentious and sizable areas, e.g. propaganda surveillance and OIS. Chapter 2 has a similar purpose to the above.

As recently mentioned, this thesis covers various intriguing yet demanding areas. Therefore, it was necessary to set out key definitions and place them within several different scenarios. This decision was taken as a means of clearing up any confusion on what keywords such as OS meant within the context of my research. Establishing clarity from the start has been achieved by assembling the thesis in such an informative way.

Chapter 3 has a similar aim in Chapters 1 and 2. Beyond defining and briefly placing keywords and concepts into particular examples, it was necessary to set out the historical evolution of propaganda and surveillance. The advantage of doing so meant that readers would have a clear grasp of the evolving nature of propaganda and surveillance. Moreover, at this stage, readers should be able to understand the importance of intelligence operations from a Western perspective, which has historically had an impact throughout the world. Also, this chapter identifies the hypocrisy of Western states that cry foul at nations such as Russia for wielding propaganda and surveillance measures. Highlighting the extensive nature of propaganda and surveillance that comes from Western countries such as the UK and US is an important task to undertake in order to convey the necessity for future researchers to build on my work and extend the current focus from Russia to Western nations.

Chapter 4 encompasses a thorough and vast literature review. While it is tempting to try and turn over every stone in search of more and more intelligence operations covered by academics, I have focused on critical areas that relate to this thesis. Cognisant of the fact that this thesis aims to dissect propaganda and surveillance, two paradoxical necessary evils, it was vital to assess what other academics have underscored concerning both subjects. Juxtaposing key issues such as ethics and intelligence paved the way for me to discover that the former is deemed to be a paradox (see chapter 4). This concept (ethical paradox) is at the centre of Chapter 6. Furthermore, other key concepts such as OS was assessed within Chapter 4 to give readers a comprehensive understanding of the term and its new place within IR, propaganda and surveillance.

Chapter 5, 6, 7, and 8 encompass the critical case studies that help to address the aims and objectives of this research. Firstly, Chapter 5 covers the temporal sequence of events starting with the release of GCHQ's international propaganda ambitions followed by the increase in offensive intelligence threshold by Russia. The response by US Congressmen and women to the alleged Russian interference was transcribed and analysed to understand the potency of OIS. To progress discussion, Chapter 6 follows immediately to address the issues of Western democratic states engaging in covert propaganda. Chapter 6 encompasses a vital case study that reveals the nature of the FBI's fake terrorist website.

Furthermore, this case study underscores the psychological impact of such a scheme in order to make it clear that the person in question, Abdella Tounisi, was potentially entrapped, thus raising concerns about the conduct of states in cyberspace. Chapter 7 and 8 covered similar themes. Chapter 7 assesses the public's ability to understand propaganda. I adopted Lippmann's stance that the public is a phantom – incapable of clear thought on abstract topics such as governance and international affairs. The phantom public as a concept was juxtaposed with what the Citizens Lab have referred to as tainted leaks. Tainted leaks is a propaganda and surveillance campaign. In relation to the particular case investigated by Citizens Lab, tainted leaks consisted of documents that were stolen by alleged Russian hackers, edited digitally then released online. Similar attempts were made during the 2017 French presidential elections, by alleged Russian hackers. This case study was vital as it allowed me to juxtapose the excessive level of OIS witnessed in the US in Chapter 5 and the lack of OIS experienced by the French public due to tainted leaks.

This juxtaposition also enabled me to conclude the usefulness of a concept such as the phantom public concerning propaganda and surveillance campaigns. Lastly, Chapter 8 capped off this quest to study OS concerning propaganda and surveillance campaigns. This case study focused on scrutinising the danger that exists when state covert propaganda and surveillance measures are revealed to the world. Each case study encompasses its analysis section or is interwoven with the details of how this case study came to be. Following the four case studies is the conclusion, which summaries the key research aims and objectives of this thesis. I have written a cross-case study section to

cover what has been written. Furthermore, the conclusion covers how this thesis has contributed to academia.

---

## Chapter 2: Definitions and Context

---

This chapter sets out to highlight and explain the key terms and theories that will be used throughout this thesis. To be clear, this chapter acts as an auxiliary tool that will help the reader understand the extensive literature in impending chapters. It is vital to underscore key concepts in this section to help shed light on issues concerning propaganda and surveillance.

The international arena is managed by states who use propaganda and surveillance as a form of social and international control. Monitoring foreign affairs and possessing the capacity to influence the decision making and thought process of foreign politicians and their citizens is crucial for nations that aim to shape the international arena. Understanding multiple ideological currents within the body of IR theory in conjunction with propaganda and surveillance is vital in order to grasp key talking points throughout this thesis. Chapter 2 sets out to underscore various crucial concepts that are directly and indirectly used throughout this. This process is of great importance as state and non-state groups have made concerted efforts to influence international affairs by capitalising on propaganda and surveillance measures. Also, chapter 2 sets out to briefly emphasise and justify the case studies that have been chosen to help address the aims and objectives set out in chapter 1.

Russia, for example, has been introducing robot trolls to cyberspace to alter and drown out the narratives of foreign policy issues throughout Eastern Europe (Helmus et al., 2018, p.25; Jaitner, 2015, p.93). Similarly, revelations concerning the USG's ZunZuneo program highlighted America's plans of warping perception in Cuba, through a smartphone Twitter-like app that Cubans had begun using. This would allow US operatives and native Cubans to communicate and exchange ideas. Detailed in Dr Brian Klaas's controversial book, *The Despot's Accomplice: How the West is Aiding and Abetting the Decline of Democracy*, Klaas suggested that the ZunZuneo program endeavoured to build a big enough following until amidst social unrest, developers of the

app could influence and direct a “smart mob” to overthrow the Cuban regime (2016, p.49). Cubans who were using the app were unaware of its origin in conjunction with the USG’s intentions to covertly spread pro-Western messages in Cuba.

Furthermore, the US hired the British PR firm, Bell Pottinger, to help the Pentagon create and monitor theatrical and highly edited propaganda as a means of altering the perception of Iraqis during the second Gulf War (The Bureau of Investigative Journalism, 2017). Moreover, chapter 1 highlights the great extent to which GCHQ went to, to have its covert unit, JTRIG, attempt to manage the perception of Argentinians on the status of the Falkland Islands and regime change in Zimbabwe and Iran (see chapter 1).

Evidently, propaganda and surveillance are being used as a covert means of self-help, to protect the national interest in an anarchic environment that has no supranational coercive body that can decisively and objectively resolve disputes (Havercroft and Prichard, 2017, p.252; Evans and Newnham, 1998, p.465; Heywood, 2011, p.54). Within the field of cyberspace, some states are reluctant to cooperate and bring an end to the anarchic terrain despite the apparent benefits that a stable cyber environment would bring to citizens and states. There are instances in which nations cooperate to bolster state and interstate security.

For example, Five Eyes is an Anglophone international intelligence alliance between Britain, America, Canada, Australia, and New Zealand. Five Eyes enables the states mentioned to carry out joint intelligence operations, share vital sensitive information concerning national threats and offensive and defensive intelligence (Gallagher and Hager, 2015; Greenwald, 2014[b], p.108; Masco, 2017, p.397; Medium, 2016; Fidler, 2015, p.200). Unsurprisingly, the anarchic environment that exists has fostered the deep sense of mistrust to which Five Eyes has responded by engaging in offensive intelligence operations against global powers such as China.

Thanks to Edward Snowden the world was alerted to the fact that New Zealand's intelligence unit, Government Communications Security Bureau, (GCSB) planned to collaborate with the NSA to spy on China (New Zealand Herald, 2015). According to one leaked document ‘GCSB has identified an MFA data link between the Chinese consulate and Chinese Visa Office in Auckland. NSA and GCSB have verbally agreed to move

forward with cooperative passive and active effort on this link. Formal coordination had begun on both sides' (New Zealand Herald, 2015). In this scenario, it would appear that cooperation was not congruent with liberal cosmopolitanism but rather with Realist talking points such as national interest, anarchy, self-help and offensive Realism.

Propaganda and surveillance measures are used to help nations to manoeuvre effectively through the international arena to gather intelligence and shape perception to benefit the national interest of a state. IR is shaped by propaganda and surveillance, although it is important to stress that the aforementioned tools (propaganda and surveillance) are not the only forces that shape IR. Moreover, considering that post WW2, states such as the US 'realised that it would take too long to transform a peace economy onto a war footing, American leaders chose to position the nation in a situation of constant heightened military preparedness'; surveillance of vast terrains around the world have become crucial to military preparedness (Haggerty, 2006[a], p. 252). Surveillance is vital for military planning for the US to help influence and control multiple spheres of influence and globally contested areas. In light of the fact that the international arena is managed by states who use propaganda and surveillance as a form of social and international influence, it is essential to cover and underscore fundamental IR theories in this thesis.

Moreover, for the sake of clarity, it is vital to accentuate that the ideological crux of this thesis is predicated on the school of Realism. Liberalism or liberal inspired concepts such as the DGC is also of great importance to help provide scrutiny to Realist assumptions in this thesis (Smith, 2017[a]). Before progressing forward past chapter 2, it is key to briefly un-pack fundamental concepts such as Realism and Liberalism due to the fact that both theories will be used throughout this thesis. Realism and Liberalism will be dissected and explored further into this thesis.

Furthermore, it is also of great importance to highlight additional concepts such as cosmopolitanism and the DGC, cyberspace, intelligence, cybersecurity, cyber espionage and cyber-attacks, surveillance and mass surveillance, propaganda, the sham universe and the democratic proselytisation of terrorism, risk, OIS and tainted leaks. All of these concepts will be used throughout this thesis; therefore, it is imperative to establish a clear understanding of the concepts mentioned above. The purpose of chapter 2 is to provide a clear link between the issues discussed in chapter 1 to the forthcoming concepts that will

be used to dissect the case studies in chapter 5, 6, 7 and 8 as well as elements of chapters 3 and 4. Moreover, concepts such as mass surveillance will be un-packaged in order to provide insight and clarity to the current surveillance culture in the West (US and UK) that has created existential privacy concerns.

Although mass surveillance is not a fundamental feature in the case studies discussed, the culture and concerns which have permeated discourse in Britain and America as a result of mass surveillance, have impacted the contextual environment of the incidents in the case studies used. For example, post-Snowden, the concern of mass surveillance has incited concerns of a big brother state that seeks to contort and control information, potentially for sinister reasons.

Moreover, once the aforementioned concepts have been un-packaged and explained, there will be a greater sense of understanding before chapter 3 and 4 begins. Chapter 3 underscores the evolution of propaganda and surveillance which thoroughly places propaganda and surveillance in context with past and modern examples of how American and British intelligence services have made use of propaganda and surveillance to shape spheres of interest and influence. Also, chapter 4, consists of an extensive and robust literature review that grapples with the litany of scholarly assumptions and interpretations of propaganda, democracy, ethics, privacy and intelligence, surveillance and OS, albeit from a Western (US/UK) perspective. Having covered a vast amount of literature and historical instances which underpins the theoretical and contextual scope of research inquiries and interest set out in chapter 1, readers will be equipped and ready to proceed to the case studies provided in chapter 5, 6, 7 and 8. However, it is of great importance to briefly highlight why these particular case studies have been chosen and how they fit into the previously discussed research inquiry (see chapter 1).

Firstly, it is important to note that while I acknowledge the relevance of liberal tenets such as cooperation that have the potential to circumvent or dissolve Realist notions such as anarchy and self – help, the predominant theoretical lens used to dissect this thesis is Realism. Case study 1 (chapter 5) highlights (as previously mentioned) the consequences of GCHQ's international endeavours being leaked online to the world. Since the Snowden leaks in 2014 which revealed that GCHQ uses covert measures to target nations such as Iran, Zimbabwe, Russia and Argentina, other countries have engaged in similar forms of



international cyber dirty tricks (see chapter 1). As a consequence, nations such as the US have become a victim of cyber dirty tricks allegedly secreted by Russia. Subsequently, the OS of some US Senators has been ruptured by Russia's litany of dirty tricks.

This chapter seeks to demonstrate that when one state attempts to mitigate its own OIS and place itself in a favourable international position, it can have a cascading effect which in the case of chapter 5, was the presence of OIS in three prominent US Senators. Online dirty tricks that are used to target international adversaries across great geographical distances are replicated and used by other states, which causes great confusion concerning the authenticity of information due to the litany of states that have chosen to poison the well with propaganda. Analysing and highlighting the degree to which US senators were gripped by OIS serves to highlight the risk and impact of modern cyber dirty tricks concerning the concept of OIS. This combination of focus is seldom a point of reference within academia. Therefore, it is of great importance to provide insight into how OS is rhetorically presented during times of crisis by political figures that are aware of recent or ongoing international influence campaigns.

Secondly, case study 2 (chapter 6) was critical to this thesis. Case study 2 was the flagship chapter that addressed the highly controversial tactics used by the FBI to catch people that gravitated towards terrorist ideation. The FBI created a fake terrorist website and left an email address at the bottom of the website to communicate with those that were interested. Subsequently, a young 18-year-old, Tounisi, emailed the fake terrorist account and sought advice on how to travel to Syria to fight on behalf of Jabhat al-Nusrah. The FBI, who was posing as Jabhat al-Nusrah recruiters, offered to pay for Tounisi's bus ticket to travel and assured Tounisi that he would receive military training to kill people in Syria.

Ultimately, Tounisi was detained and arrested by the law enforcement officers who spotted him at an airport trying to fulfil the FBI's plan of travelling to Syria. When considering the extensive information provided about this particular case in chapter 6 (see chapter 6) it becomes questionable as to whether or not Tounisi was entrapped by the FBI and in conjunction with the possibility that the FBI produced war propaganda which violates article 20 of the International Covenant on Civil and Political Rights (OHCHR, 2019[a]).

Questions of possible human rights violations have been addressed in order to understand the far-reaching implications of online propaganda and surveillance methods. Case study 2 is vital to this research because it presents modern propaganda and surveillance methods that are conducted online by prominent US intelligence services such as the FBI. Moreover, case study 2 also offers an insight into the danger and risk of citizens to become victims of OIS should they learn that intelligence services from democratic nations have reneged on their liberal ontology and sought to proselytise terrorism in cyberspace covertly.

Thirdly, case study 3 (chapter 7) looks at the combination of propaganda and surveillance measures that are wielded by the non-state group CyberBerkut. CyberBerkut is believed to be working on behalf or in association with the Russian government, although this association has not been unequivocally proven (Hulcoop et al., 2017). This study was crucial because it addressed Lippmann's concept of a phantom public that undermines the ability of the public to comprehend society and successfully take part in a democracy other than to vote politicians into power (Lippmann, 1993, p.58-59).

Essentially, Lippmann paints a dim picture for society and its citizens that are incapable of being omniscient, rational and enthusiastic enough to master the totality of government affairs. As a consequence, propaganda is required to shape public opinion and guide citizens to the *correct* conclusion. In light of the fact that 20<sup>th</sup>-century propaganda has been persuasive enough to encourage citizens to go to war and in other instances commit mass genocides, contemporary digital propaganda that is advanced by modern technological sophistication can be harder to detect.

In order to theoretically assess the capability of modern citizens amidst modern propaganda and surveillance endeavours, I have selected the case study of tainted leaks and the French elections that were subject to information operations by the non-state group Pawn Storm (that is believed to be a cover name by the Russian government). With regards to the former, i.e. tainted leaks, CyberBerkut a non-state group, hacked into the email account of an investigative journalist in order to search for sensitive documents, steal them, edit the contents and release the final product to the world as a genuine leak (Hulcoop et al., 2017). This has been referred to as tainted leaks by Citizens Lab, who

carried out the forensic investigation on behalf of Satter and publicised the information campaign by CyberBerkut. Russian state news stations aired these leaks as truths.

Moreover, I have analysed the incident of tainted leaks concerning the phantom public to assess the extent to which the public can withstand and understand propaganda and surveillance campaigns. Similarly, the subcase study of the 2017 French presidential elections consisted of a Russian linked non-state group, Pawn Storm, that hacked into President Macron's election campaign network (Auchard, 2018; Trend Micro, 2017). Sensitive documents were stolen, edited, then released to the public as a legitimate leak (Auchard, 2018; Trend Micro, 2017).

I assessed the reasons why this tainted leaks attempt was unsuccessful, which refutes some of Lippmann's claims about the alleged phantom public. Overall, both incidents studied in case study 3 were utilised to address the research aim and question of; is it permissible to refer to the public as a phantom public that is ill-equipped to deal with sophisticated or rudimentary cyber propaganda manoeuvres postulated by intelligence services and non-state groups? Furthermore, amidst the confusion and potential inability to detect and classify information as propaganda, can mistrust of information produce OIS that curtails the willingness of citizens to hold strong opinions? This is a fundamental research aim and question that is addressed by assessing tainted leaks, the French elections in conjunction with the phantom public.

Finally, case study 4 (chapter 8) is a fundamental section of research that serves to highlight the consequences of modern propaganda and surveillance measures. Public trust in conjunction with OS, can plunge as a result of revelations about sinister theatrical propaganda that is being created and utilised by Western democratic governments. Case study 4 is predicated on revelations that British PR firm Bell Pottinger created theatrical and highly edited propaganda in order for the US to puncture support for Al-Qaeda in Iraq during the second Gulf War. US soldiers dropped CD's that contained Bell Pottinger's edited propaganda, during house raids in Iraq (The Bureau of Investigative Journalism, 2017). The CD's contained a code that allowed the US to track the location of where people were watching the video via google analytics (The Bureau of Investigative Journalism, 2017). Years after this scandal, Russia accused the West of creating Hollywood propaganda consisting of staged psychological warfare, i.e. fake

videos of Syrian government victims of gas attacks (see chapter 8). The danger of using black covert propaganda is that once it is exposed, adversaries can concoct spurious claims which are no longer outlandish because they are predicated on the recent memory of, for example, the US engaging in propaganda and surveillance measures in Iraq.

This research endeavours to address the gap in knowledge concerning current surveillance and propaganda methods that make up JTRIG's playbook of dirty tricks. Specifically, the first research aim is to demonstrate that attempts by states to mitigate OIS, can have a counterproductive effect in a Realist environment that pushes competitive states into engaging in high-risk cyber intelligence operations, which in turn increases OIS. Put in another way, OIS among states is amplified by their clandestine intelligence activities that end up being replicated by other states once such measures become public knowledge. Once the information environment has been infected by a considerable amount of propaganda, the truth looks similar if not identical to a lie, which has the potential to thrust citizens into a state of OIS concerning issues within domestic society and IR.

---

## 2.1 An overview of Realism and Anarchy

---

World history is riddled with both cooperative acts simultaneously submerged under numerous examples of destructive state competition and excessive violence. In 1898 Britain threatened the use of force against a French garrison in Fashoda Sudan, as a means of removing colonial competition (Chafer, and Cumming, 2010, p.1130). Decades later during the Cold War, the US considered a devastating attack on the Sino-Soviet bloc to 'remove the enemy from the category of a major industrial power' (National Security Archive (US), 2018, p.9). Fast-forward to the 21<sup>st</sup> century 'British soldiers from 1st Battalion [t]he Royal Welsh have deployed to Estonia' to deter Russia (Ministry of Defence (UK) and Fallon, 2017). Collectively, racist, genocidal, expansionist nations and empires, settler states, post-colonial saturation of French military power in black Africa, subversive US 'Covert Actions', has been an existential nightmare for much of the world's population (Chafer, 2005, p.7-10; Davis, 2001, p.26-28; Office of the Historian, n.d.[b]; Perez, 2008, p.4-5; Pihama, et al, 2014, p.250; Vallin, 2015, p.79; Wolfe, 2006, p.62). To compound this sizable list even further, contemporary international propaganda

and surveillance campaigns have infringed upon the privacy of citizens across the globe (Fishman and Greenwald, 2015; Greenwald, 2014[b], p.92-93).

States often find themselves locked in a regional or global competition for power and security. This gloom assessment has led to the theory of Realism, which attempts to explain state behaviour in terms of power politics and destructive human behaviour that influences reactionary (government) domestic and foreign policy. To a great extent, Realism is the dominant theoretical driving force of IR. Peter Hough has defined IR as ‘the study of all political interactions between international ‘actors’, which include: states (represented by governments), international organisations (either inter-governmental or non – governmental) and, to a lesser extent, some influential private individuals’ (2018, p.1).

Within IR theory, Realism has ‘dominated the study of security and focused inquiry on military security in inter-state relations’ (Hough, 2013, p. 21). Realism is defined as a broad intellectual ‘school of thought that explains international relations in terms of power’ (Pevehouse and Goldstein, 2013, p.38). However, it is important to note that Realism has evolved over time. Although the Realist school of thought revolves around the basic principle of power politics, security and conflict, various strands of Realist perspectives have emerged. Classical Realism, Neo-Realism, defensive Realism and offensive Realism are examples of the diverse approaches of analysing the world and interstate behaviour. <sup>4</sup>

To begin with, defensive Realism like its theoretical cognates revolves around the notion of power but assumes that security or at least the temporary sense of security can be assured by maintaining a balance of power among states. Defensive Realism is a theory that emphasises the maintenance of power among states to produce a relative sense of security, as opposed to making adversaries and allies concerned about a nation that seeks to maximise power beyond reasonable levels (Blanton, and Kegley, p.27). As such, nations seek to establish what Realists refer to as a balance of power. A balance of power among states would foster a multipolar environment as opposed to one single superpower or bloc directing world affairs (Blanton and Kegley, 2017, p.25). In contrast, offensive

---

<sup>4</sup> Neo Realism is explained further down in the chapter.

Realism purports that the world is subject to anarchy; therefore, it is logical for states to maximise power to establish a sense of security. Without a unilateral objective force to subject all states to the same set of rules that would deter aggression, states cannot trust each other. Consequently, nations are tempted to expand military and security forces domestically and internationally to repel potential threats (Wohlforth, 2010, p.139). To be precise, offensive Realism can be described as a ‘variant of realist theory that stresses that, in an anarchical international system, states should always look for the opportunities to gain more power’ (Blanton, and Kegley, 2017, p.27). Offensive Realism is thus theoretically in line with the Realist concept of *anarchy*; which will be explored further down in this section.

Offensive Realism’s chief proponent John Mearsheimer has suggested that ‘[g]enuine peace, or a world where states do not compete for power, is not likely’ (1994, p.9). Peace and unilateral cooperation are not likely to occur because states are preoccupied with the threat of war ‘always in the background’ haunting the calculations of other nations (Mearsheimer, 1994, p.9). Joseph Grieco denotes a similar conception of Realist thought in highlighting that ‘states worry that today’s friend may be tomorrow’s enemy in war, and fear that achievements of joint gains that advantage a friend in the present might produce a more dangerous potential foe in the future’ (Grieco, 1988, p.487). To this end, an environment akin to Realist conditions is saturated with real, potential and farcical perceptions of the future which pushes states into destructive acts of violence towards other nations and their citizens in the name of maximising security and peace.

Pivoting back to classical Realism, this theoretical strand is grounded in juxtaposing the reactionary and destructive element of human nature with the systemic violent habits of states. According to Andrew Heywood, classical Realism is predicated on the assumption that IR and power politics can be explained by reflecting upon human selfishness and an overall eagerness for individuals to pay greater interest to their safety and prosperity over the wellbeing others nations (Heywood, 2011, p.54). Additionally, Heywood asserts that Classical Realism ‘explains power politics in terms of egoism’ (2011, p.54). Egoism is defined as the ‘[c]oncern for one’s own interest or wellbeing, or selfishness; the belief that one’s own interest are morally superior to those of others’ (Heywood, 2011, p.54). Within classical Realism, Egoism is a prominent factor of human nature and IR, which

leaves states inexorably bound to conflict or the threat of conflict. As suggested by Waltz ‘[a]mong states, the state of nature is a state of war’ (Waltz, 1986, p.98).

Furthermore, classical Realism assumes that the present is subject to the cyclical mistakes of the past. Humans and states are thus incapable of moving beyond repeated threats and acts of violence, even if cooperation and peace are a realistic and viable option. A great deal of this theoretical ‘pessimism is rooted both in human nature and the international system’ (Mastanduno, 1999, p. 20). Due to the assertion that ‘[v]irtually everyone is born with a will to power hardwired into them, which effectively means that great powers are led by individuals who are bent on having their state dominate its rivals’ fear and suspicion of other nations is prevalent in IR (Mearsheimer, 2013, p.77).

The theoretical antecedents of classical Realism is predicated on the brutal and reactionary aspect of human history. Prominent figures from the past such as Thomas Hobbes, Niccolò Machiavelli and Thucydides have attested to the stark issue of human nature, which drives states into direct military conflict. Ideologically, Machiavelli was bound to an obtuse Realist theoretical perception of human nature and the need for cynical tactics to ensure the maintenance of power:

*A ruler, then, should have no other objective and no other concern, nor occupy himself with anything else except war and its method and practices, for this pertains only to those who rule... on the other hand, it is evident that if rulers concern themselves more with the refinements of life than with military matters, they lose power. The main reason why they lose it is their neglect of the art of war; and being proficient in this art is what enables one to gain power* (Machiavelli, 1993, p.51-52).<sup>5</sup>

Moreover, Thucydides, an Athenian historian, has had a long-lasting impact on Realism. Thucydides recollection of the Peloponnesian conflict identifies what most modern proponents of Realism identify as common denominators for wars and global instability: fear and the loss of state power. Upon assessing the variables that pushed Sparta and Athens go to war ‘the growth of the power of Athens, and the alarm which this inspired

---

<sup>5</sup> I am aware that Realism was coined after Machiavelli.

in Lacedaemon, made war inevitable' (Thucydides, 2013). Fear of other nations and civilisations have driven governments to embrace offensive manoeuvres in cyberspace irrespective of the risk to international stability or cybersecurity.

Lastly, within realism 'states are the principal or most important actors in an anarchical world lacking central legitimate governance. States represent the key unit of analysis' (Viotti, and Kauppi, 2010, p. 42). By this principle, institutions such as the International Court of Justice (ICJ) are not integral to IR. Instead, IR is shaped by nations. Put bluntly by Viotti, and Kauppi '[r]ealists tend to see international organizations as doing no more than its member states direct' (2010, p. 42). Looking back at US self-declared concepts such as exceptionalism, the UN was also unable to restrain Washington's flagrant disobedience and disregard for the ICJ during the Cold War. After it was revealed that the US was sponsoring 'Paramilitary Activities' to overthrow the Nicaraguan regime, in 1984 the nation of Nicaragua took America to the ICJ (ICJ, 2010). Unsurprisingly, the court ruled in favour of Nicaragua, declaring that:

*[T]hat the United States was under a duty immediately to cease and to refrain from all acts constituting breaches of its legal obligations, and that it must make reparation for all injury caused to Nicaragua by the breaches of obligations under customary international law (ICJ, 2019).*

The international community has been unable to force the US to recognise the ruling and authority of the court. Since this global fiasco, the US has invaded Iraq on two separate occasions, launch airstrikes on Serbia and Libya, invaded Afghanistan, occupied parts of Syria and maintain naval fleets in Latin America, the Far East, Europe and the Middle East to intimidate other states. Most, nations, particularly powerful nations, adhere to the Realist theoretical notion that 'power is the currency of international politics' (Mearsheimer, 2013, p.77).



---

## 2.2 Anarchy

---

A key tenant within the theory of Realism and this thesis is anarchy. Overlapping foreign policy, aggressive state desire for expansion of influence, and the lack of a supreme, coercive and unilateral overseeing force that acts above all states, has encouraged a variety of authors to suggest that the world is in a state of ‘anarchy’ (Lechner, 2017, p.341-342; Williams, 2009, p.328; Mearsheimer, 2013, p.79; Waltz, 1986, p.98-99). The concept of anarchy can be traced back to writers such as Hobbes who associated the former with a lack of an overseeing force to compel human beings.

In *Leviathan*, Hobbes depicts the crude nature of humankind that is inexorably bound to strife due to a lack of regulation by a supreme unilateral power (1994, p.88). As put by Hobbes ‘men live without a common Power to keep them all in awe, they are in that condition which is called Warre; and such a warre, as is of every man, against every man...therefore the notion of *Time*, is to be considered in the nature of Warre’ (1991, p.88). If the interpretation by Hobbes is correct, states will maintain standing armies, ready to inflict death upon international adversaries because there is no unilateral unchallengeable power that can intervene on behalf of states to restore an objective sense of order.

At its basic form ‘anarchy is the absence of rulers, of a centralised authority or a system of self-help’ (Havercroft and Prichard, 2017, p.252). Anarchy is a concept that is widely enshrined in the ‘self-image’ and discourse within IR (Havercroft and Prichard, 2017, p.252). A definition of anarchy that I feel is synonymous with the drive behind this thesis and the current state of cyberspace suggests that anarchy is the lack of a ‘hierarchically superior, coercive power that can resolve disputes, enforce law or order the system of international politics’ (Karatzogianni and Robinson, 2017, p.282-283). Similarly, sovereignty has been defined as ‘[a] states right, at least in principle, to do whatever it wants within its territory; traditionally, sovereignty is the most important international norm’ (Pevehouse and Goldstein, 2013, p.43).

However, there is a need to differentiate between domestic and international sovereignty. Andrew Jones has focused on a nations domestic remit of sovereignty in suggesting that ‘[a] sovereign state is thus one that is free and independent and in its internal affairs has

undivided jurisdiction over all persons and property within its territory' (2006, p.208). On the other hand, the sovereignty to act preponderantly within the international arena should also come into consideration as opposed to solely focusing on a nation's domestic remit. Evans and Newman have pointed out that '[t]he doctrine of sovereignty implies a double claim: autonomy in foreign policy and exclusive competence in internal affairs' (1998, p.504).

Often international bodies such as the EU and the UN find it challenging to make nations yield to their authority. For example, US national security advisor, John Bolton, launched a scathing attack on the ICC stating that '[w]e will let the ICC die on its own. After all, for all intents and purposes, the ICC is already dead to us' (Aljazeera, 2018). Similarly, back in 2014, the European court of justice (ECJ) ruled that it's previous Data Retention Directive 'to be invalid' (Court of Justice of the European Union, 2014, p.1). Britain, who relies on data retention for alleged national security purposes, countered this move by rushing through Parliament DRIPA, in open defiance of the EU (*Data Retention and Investigatory Powers Act 2014*, p.5).

Although DRIPA was declared unlawful by UK courts in 2018, till this day, the EU has not been able to rip up DRIPA and establish control of this specific British law (Liberty, 2018). Considering the speed at which the Conservative British government created a new law and had it enforced, it is clear that some states can and will act in open defiance of international regimes in matters concerning cyberspace and national security. To someone who subscribes to classical Realist tenets, this example demonstrates how anarchic global systems can be.

Similarly, Neo-Realists such as Kenneth Waltz pointed out the concern that states have with entrusting power into a central supranational body:

*States cannot entrust managerial powers to a central agency unless that agency is able to protect its client states. The more powerful the clients and the more the power of each of them appears as a threat to the others, the greater the power lodged in the center must be. The greater the power of the center, the stronger the incentive for states to engage in a struggle to control it (Waltz, 2010, p.112).*

If the centre of power does not intimidate states into submission, instances like DRIPA take place. Essentially, ‘when no authority exists that can enforce agreements – “anarchy” – then any state can resort to force to get what it wants’ (Wohlforth, 2010, p.135). On the other hand, it is crucial to note that Realist conceptions such as anarchy have been refuted on the basis that the international system is not in disarray but subject to a limited amount of hotspots that occasionally impact a nation's perspective. Athina Karatzogianni and Andrew Robinson have indicated that ‘[t]he state perceives chaos or (bad) anarchy, not because there is no order, but because this order is incompatible with the state’s own existence’ (2017, p.284). Essentially, anarchy is in the eye of the beholder rather than being a definitive objective fact.

The US may perceive the world in terms of anarchy because of its global remit to interfere in the affairs of foreign nations. Realism and anarchy can thus be construed as ‘a toxic concept in IR theory, routinely associated with conservative and retrograde politics’ which hyper inflates sensitive relations between nations (Havercroft and Prichard, 2017, p.253). Nonetheless, throughout this thesis, I will incorporate the notion of anarchy, directly and indirectly, to illustrate the current cyber terrain. Although I will make attempts to exonerate Brad Smith’s liberal concept of a DGC, ultimately the triumph of Realism in cyberspace will expose liberal tenets and help readers to understand why each case study is heavily associated with Realist theoretical undercurrents (Smith, 2017[b]).

---

## 2.3 Neo-Realism

---

Fundamentally Neo-Realists such as Waltz acknowledge the essential need to focus on state power and security fears but deviate from Classical Realism on the basis that, IR can be explained in terms of its structure as opposed to being based on the wickedness of human nature. According to Waltz ‘[d]ifferent structures permit and cause the units of a system to change their [behaviour] and produce different outcomes’ (Waltz, 2004, p.4). Waltz is attempting to suggest that global order and the balance of power is the predominant factor that alters how states behave. As such, within the international arena the:

*Impulses of a state to behave in arbitrary and high-handed fashion are constrained by the presence of states of comparable capability. An international*

*system in which another state or combination of states is unable to balance the might of the most powerful is like a political system without checks and balances* (Waltz, 2004, p.4).

Waltz's assessment, to a great extent, highlights the structural element of IR as opposed to solely focusing on human nature. Moreover, throughout the Cold War, theorists began to expand the IR scope 'beyond military power politics' to interpret the world and began acknowledging other determining factors (Hough, 2013, p.3). Neo-Realists believe that 'interstate cooperation will create institutions and regimes for the peaceful settlement of conflicts' (Simon, 1995, p.5). Hough has suggested that as a result of:

*'[E]conomic interactions between states in the 1960s and 1970s... Realist thought metamorphosized into 'Neo-Realism', which maintained the focus on states and the pursuit of power but accepted that not everything happens in the world is determined by military might. States could become powerful by concentrating on their economies (such as West Germany and Japan)* (Hough, 2013, p.3).

In the 21st century, this is exemplified in the growth and international expansion of Sovereign Wealth Funds (SWF). Norway, in particular, has become an economic powerhouse with a SWF that reached \$1 Trillion in 2017 (McCarthy, 2017; Solsvik and Fouche, 2017). SWF has enabled Norway to accumulate global financial influence or soft power, with significant investments ranging from Latin America, Africa, Europe and Asia (Norges Bank Investment Management, 2018). Moreover, despite US and EU sanctions levelled at Russia, its Direct Investment Fund (SWF) has worked with SWF and investment bodies of other nations to secure investment that contributes to development in other nations as well as Russia.

To be precise, Russia has partnerships in the form of a '\$2 billion Russia-China Investment Fund, 70% of which will be invested in Russia' with the collaboration of the China Investment Corporation (CIC) (Russia Direct Investment Fund, 2018). Strands of Neo-Realism thus manifests in the form of international cooperation and interaction, with the state still as the referent object, alongside economic forces. Having acknowledged this, I still argue that states will display offensive Realist tendencies of aggressive competition in private and public while simultaneously entertaining liberal cooperation

to fulfil the status quo of behaving like a normal law-abiding state (see chapter 8). The spoils from infiltrating the networks of another state are too sweet of fruit to engage in respectful international cooperation seriously.

Realism, as a theory contains various theoretical strands. This thesis, in general, will oscillate between various concepts and approaches within the Realist school of thought. However, within this thesis, I argue that cyberspace is in a state of anarchy to which nations will not consistently or meaningfully feel compelled to cooperate with adversaries peacefully. This is a result of the technological developments in intelligence services and private companies that help states to covertly surpass their adversaries while claiming to be open to cooperation. Offensive Realism is more theoretically aligned with my claim; however, this does not rule out acknowledgement or acceptance of various other subgroups within the school of Realism. The term Realist will, therefore, be used when referring to this (offensive Realism) description. When a particular example or passage requires a specific theoretical demarcation, I will mention the particular strand of Realism that I am referring to.

---

## 2.4 Liberalism

---

Liberalism is an ideological counterbalance to theories such as Realism that are and have been the ideological driving force within IR. Liberalism is predicated on the assumption that nations are ‘rational actors driven by their interest would see the merits of peace and prosperity, which makes cooperation possible and sustains order’ (Srivastava and Sharma, 2017, p.23). While Realists purport that states are driven by selfish national interest that at times prohibit the possibility of cooperation, liberals generally view the world in a far more positive manner. In the view of Robert Jackson and Georg Sørensen ‘Liberals generally take a positive view of human nature. They have great faith in human reason and they are convinced that rational principles can be applied to international affairs’ (2016, p. 97).

This positive view is predicated on the various measures or checks and balances that can be implemented by liberals to restrain state aggression. Institutions, for example, can create a network of interdependence that help to limit the degree of inter-state violence.

For instance, during the Venezuela debt crisis of 1902, Britain, Italy and Germany sent warships to implement a naval blockade around Venezuela as a means of forcing all debts to be settled (Maass, 2009, p.388).

In the 21<sup>st</sup> century during the Greek debt bailout crisis, no warships were sent to by EU member states to force a final capitulation by Greece to the demands of the International Monetary Fund (IMF), private lenders and the EU. The various layers of interdependence between institutions such as the EU, the European Commission (within the EU) and the IMF, (which is an institution within the UN) enables states to resolve their disputes without turning to acts of aggression (IMF, 2019). Economic interdependence, as well as the diplomatic networks and legal boundaries that have been created by the aforementioned institutions, is not an unequivocal deterrent to the commencing of hostilities but rather a significant buffer that helps states to resolve issues peacefully. For this reason, liberals take the view that war is not inevitable.

Furthermore, Realism diminishes the role that non-state actors and institutions play within IR. Realists view states as the most important units within IR, while simultaneously ascribing a diminutive and non-influential role to non-state groups. In contrast, in Robert Keohane and Lisa Martin infamous rebuttal to John Mearsheimer critique of Liberalism *The False Promise of International Institutions*, Keohane and Martin emphasised empirical findings which demonstrated the importance and value of institutions within IR. Keohane and Martin have rightly pointed out that nations have made significant ‘investments... in such international institutions as the EU, NATO, GATT, and regional trading organizations’ (1995, p.47). In fact, when President Macron referred to NATO as brain dead, multiple NATO members were quick to rebuke this comment and alluded to the importance of integration via institutions (NATO) (Rose, 2019).

Within Liberalist theories, international non-state or intergovernmental organisations can play a role on the world stage to aid interstate cooperation and help states with security issues. As will be discussed further down in this chapter, the UN has been an organisation that has had an ambivalent impact on the world stage. Additionally, much smaller organisations such as MAG ‘find and destroy landmines, cluster munitions and unexploded bombs in places affected by conflict’ (n.d.,[a]). A testament to Liberalism is the fact that MAG receives donations and support from the US Department of State, UK’s

Department for International Development, New Zealand's Ministry for Foreign Affairs and Trade (Aid Program) and Norway's Ministry of Foreign Affairs (n.d.[b]). To a great extent, Liberalism does work, and non-state groups can help to contribute to peace. The issue within IR is the length of time this form of cooperation can last?

Essentially, non-state actors do matter. For this reason, it can be construed that the Realist marginalisation is irrational and not predicated on empirical evidence. Rather, the real-world manifestations of liberal tenets are indicative of the assessment that 'Liberalism has been the dominant ideological force shaping western political thought' (Heywood, 2014, p.65). The ideological feud between Liberals and Realists is centred upon the extent to which cooperation that is facilitated between states can last until Realist tenets such as self-help begin to manifest as a result of the anarchic structure that causes states to renege on previous agreements. Much to the dismay of Liberalism and its advocates, President Trump has notified the UN to inform them that the US intends to withdraw from the 2015 Paris accord's in which 187 other states committed to as a means of keep rising global temperatures below 2C (BBC, (2019[d])).

On both domestic and international fronts, '[l]iberals recommend replacing cutthroat, balance-of-power politics with organizations based on the principle that a threat to peace anywhere is a common thread to everyone' (Blanton and Kegley, 2017, p.30). As such, Liberalism has been defined as:

*A paradigm predicated on the hope that the application of reason and universal ethics to international relations can lead to a more orderly, just, and cooperative world; liberalism assumes that anarchy and war can be policed by institutional reforms that empower international organization and law* (Blanton, and Kegley, 2017, p.28).

This definition is of great relevance and value to this thesis as the potential of a DGC will be used to assess examples of Realist manifestations of anarchy and self-help in cyberspace.

---

## 2.5 Liberal Cosmopolitanism and the Digital Geneva Convention

---

The ideological derivative of the DGC stretches back to Immanuel Kant's conception of cosmopolitanisms (Dockstader, 2018, p.1; Kamminga, 2017, p.2-3; Cavallar, 2012, p.97-98; Mendieta, 2009, p.242; Kant, 1983, p.29-36). Before untangling and dissecting the DGC, it is necessary to highlight its ideological roots. Cosmopolitanism typically orbits around the 'combination of universalism, humanism and communitarianism' (Dockstader, 2018, p.1). All three notions share the common theme of a liberal drive to produce equality and peace for the advancement of humankind. In saying this '[a]ll cosmopolitans believe that we should view ourselves as deeply linked to humanity as a whole' (Thomas, 2008, p.139). Cosmopolitanism intends to overcome the seemingly continual streak of human conflict by compelling states to come together under one morally conscientious peaceful organisation. Essentially, Kant acknowledges Realist concerns of anarchy but disavows the view that strife is a permanent feature of humankind and future generations.

Instead, Kant was confident that peace is an inevitable teleological process woven into the destiny of humankind. In particular, Kant suggested that 'peace can neither be inaugurated nor secured without a general agreement between the nations; thus a particular kind of league, which we might call a *pacific federation (foedus pacificum)*' is needed (1991, p.104). Cosmopolitanism can be perceived as the coming together of states on an international scale to form a peaceful bloc that intends to expand until peace is secured for all countries. For cosmopolitanism to manifest, it will require 'one powerful and enlightened nation' to:

*[F]orm a republic (which is by its very nature inclined to seek perpetual peace), this will provide a focal point for federal association among other states. These will join up with the first one, thus securing the freedom of each state in accordance with the idea of international right, and the whole will gradually spread further and further by a series of alliances of this kind (Kant, 1991, p.104).*



The League of Nations and the UN are two examples of liberal attempts to unify states to implement peace. Moreover, Kant's desire for a cosmopolitan network of states was based on his suggestion that:

*The greatest problem for the human species, whose solution nature compels it to seek, is to achieve a universal civil society administered in accord with the right... Since it is only in such a society that nature's highest objective, namely, the highest attainable development of mankind's capacities, can be achieved, nature also wills that mankind should itself accomplish this... Necessity compels men, who are otherwise so deeply enamoured with unrestricted freedom, to enter in to this state of coercion; and indeed, they are forced to do so by the greatest need of all, namely, the one that men themselves bring about, for their propensities do not allow them to coexist for very long in wild freedom (Kant, 1983, p.33).*

Freedom, a key ingredient in Kant's cosmopolitan utopia, was only freedom if it conformed to the overall security of states. That is to say, the sovereignty to pursue selfish endeavours that have pushed countries into conflict must eventually be relinquished so that nations can assimilate into a unified, peaceful body. As such, Kant highlighted that endless strife 'must force nations to just the same decision (however hard it may be for them) to which savage men were so unhappily forced, namely, to give up their brutal freedom and to seek calm and security in a law-governed constitution' (1983, p.35). However, it is vital to point out that within this federation, obedience to the law and self-restraint is not imposed by force as states abide by treaties. Instead, '[t]his federation does not aim to acquire any power like that of a state, but merely to preserve and secure the *freedom* of each state in itself, along with that of the other confederated states' (Kant, 1991, p.104).

Conversely, amidst a cantankerous bloc of states that subscribe to previously agreed regional security deals in which if one member nation is attacked all countries take some form of defensive and offensive measures, it may be challenging to assume that a group of rogue states will submit to an enlightened power and its allies. Instead, they may bask in the glory of their loyalty towards other friendly neighbours and maintain their desire to pursue hostile policies. This is another critical talking point in which the DGC may be undone by Anglophile nations such as the UK, the US, Australia, New Zealand and

Canada which comprise of the intelligence alliance, Five Eyes. Five Eyes can infiltrate the networks of other nations, notably without permission of the UN.

Moreover, Kant presents a teleological assumption which implies that anarchy is nature's way of directing man to a pure form of being, in a symbiotic matrix of peaceful, cosmopolitan states. Accordingly *'[t]he means that nature uses to bring about the development of all of man's capacities is the antagonism among them in society, as far as in the end this antagonism is the cause of law-governed order in society'* (Kant, 1983, p.31). Conflict, therefore, plays a necessary function in conditioning and shaping states to adopt and embrace peaceful instincts over malevolent domestic and foreign policies.

In an attempt to limit the impact of war and constrain state aggression, the Geneva conventions were gradually established and adopted in the 1800s and throughout the 20<sup>th</sup> century. The Geneva Conventions are a set of international treaties implemented to protect human life from warfare as a means of establishing necessary human rights protection (International Committee of the Red Cross, n.d.). In light of the anarchic cyber environment that has caused a range of issues (see chapter 3 and 4) Brad Smith, the President of Microsoft has called on nations and the private sector to create a DGC to protect citizens of all countries from malicious cyber actors.

Ideally, the DGC would 'commit governments to implement the norms that have been developed to protect civilians on the Internet in times of peace' (Smith, 2017[b]). Effectively, the DGC would compel nations and non-state actors to cease hostile activity, i.e. hacking, surveillance, theft of data in cyberspace and propaganda so that citizens can enjoy the Internet in peace. Smith has stressed that a DGC should commit to:

*[A]voiding cyber-attacks that target the private sector or critical infrastructure or the use of hacking to steal intellectual property. Similarly, it should require that governments assist private sector efforts to detect, contain, respond to and recover from these events* (Smith, 2017[b]).

Under the DGC tech companies such as WhatsApp would receive constant government support concerning vulnerabilities and the latest upgrades in network security. Intelligence services would work to bolster cybersecurity of institutions as opposed to predominantly being geared towards figuring out how to subvert networks. Without a

doubt, the DGC is an ideal concept that is integral to bringing stability in cyberspace. Unfortunately, at times liberal notions no matter how necessary they may be, fall prey to Realist impulses that push states towards destructive tendencies. The DGC will be used to assess Chapter 5, 6 and 7 in order to help emphasise the extent to which cyberspace has descended into anarchy.

---

## 2.6 Cooperation

---

Cooperation, as a term may encompass liberal undercurrents of one individual, group or state working in tandem with another person group or state for a greater cause. Instinctively, one would assume that cooperation, which is ‘[t]he action or process of working together to the same end’ would help to avert economic disaster, political strife and war (Oxford Dictionary, 2018). However, this thesis is riddled with examples and case studies which demonstrate both negative and positive dimensions to cooperation. State and non-state groups can cooperate for peaceful outcomes, albeit the term peaceful will be subject to interpretation. States often cooperate in small or sizable clusters to promote international peace through military engagement with struggling states. Within IR, multilateralism has been defined as ‘the practice of coordinating national policies in groups of three or more states, through ad hoc arrangements or by means of institutions’ which has breathed life into Liberalism (Keohane, 1990, p.731). With regards to Keohane’s definition, in 2018, France and the UK increased military cooperation with the UK pledging to:

*[B]olster a key French counter-terrorism operation in Africa by deploying three RAF Chinook helicopters to Mali... The helicopters, which will provide logistic support to French troops, are part of a wider effort to increase stability in the Sahel region of Africa in order to tackle Islamist terrorism (Prime Minister’s Office et al., 2018).*

Similarly, in 2014 France dispersed 4000 troops throughout Mauritania, Mali, Niger, Chad and Burkina Faso under Operation Barkhane to help stem terrorist and criminal activity in the region (Embassy of France in London, 2018[a]; Embassy of France in London, 2018[b]). In addition to Operation Barkhane, the 5000 strong G5 Sahel force

was officially launched on 2 July 2017 to fight ‘terrorism, cross-border organized crime and human trafficking in the G5 Sahel zone’ (France Diplomatie, 2018). Approval from international bodies such as the UN and the AU provided legitimacy to the creation of the G5 Sahel force (France Diplomatie, 2018).

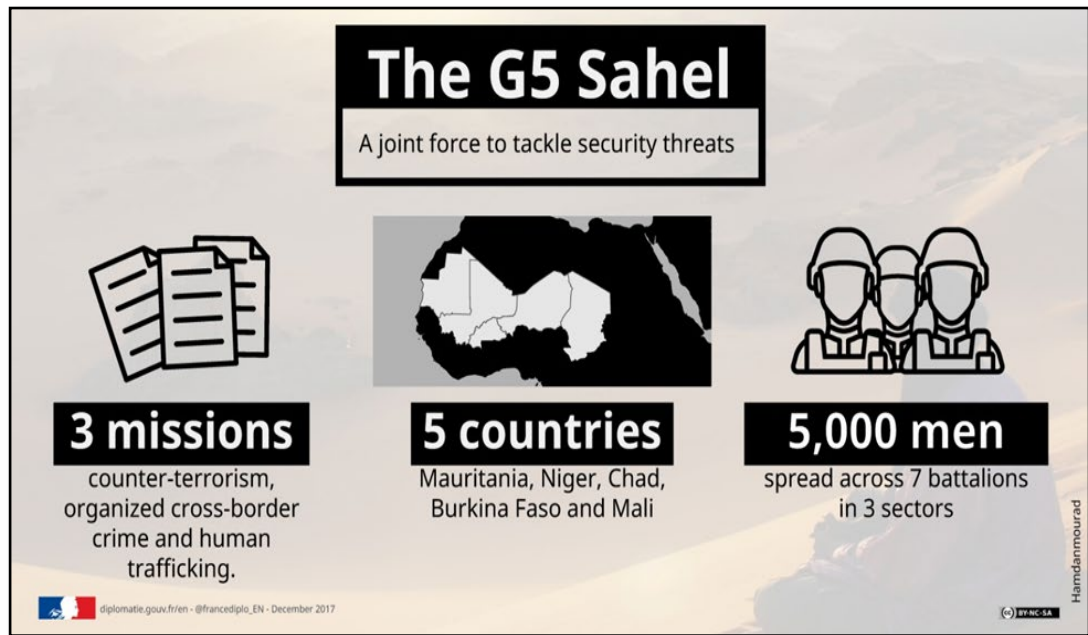


Figure 6: France Diplomatie, 2018

Conversely, the track record of the UN is not impeccable despite its capacity to facilitate cooperation. Back in 2013, France and UN peacekeeping forces intervened in the Central African Republic to stem mass killing. The UN was rocked by a scandal involving French soldiers that engaged in sexual acts with children. Anders Kompass, a UN aid worker exposed the scandal as a last resort after he felt the UN was not taking the issue seriously, was placed on administrative leave, which incited accusations of a cover-up (Esslemont, 2016). According to Kompass, the complete impunity of the those in the UN that have abused their power, concerning the sexual abuse of children in the Central African Republic, made it impossible for him to keep working for the UN (Anyadike, 2016). Additionally, the UN’s approved a no-fly zone in Libya, which authorised member states ‘to take all necessary measures to protect civilians under threat’ (UN, 2011). This measure helped to facilitate the eventual collapse of the Gadhafi regime, plunging the nation into an ongoing civil war (UN, 2011).

Furthermore, the context of international cooperation during the period of colonialism can be interpreted as opportunistic and unfair. In 1901 during the Chinese Boxer Rebellion, nationalist entities called ‘I-ho-ch'uan (the Righteous and Harmonious Fists)’ or ‘boxers’ grew resentful towards the presence of Westerners and began to launch deadly attacks against missionaries (Australian War Memorial, n.d.). Before this uprising, imperial China had suffered multiple embarrassing losses in warfare, which forced the celestial dynasty to seek concessions to its foes. Two Opium wars launched by the British and military incursions by the French to wrestle control of Tonkin (Vietnam) which eventually became a part of the French empire or French-Indochina, had strategically set China back (Lovell, 2012, p.14; Munholland, 1981, p.629-630).

At prominent trading places such as Shanghai, ‘French, German, British, and American merchants demanded large tracts of land in which they asserted "extra-territorial" rights - being subject to the laws of their own country rather than Chinese law’ (Australian War Memorial, n.d.). Driven by humiliation, Empress Dowager eventually sided with the boxers and took up arms against Europeans. In response to a multitude of attacks by the boxers ‘Great Britain, Germany, Russia, France, the United States, Japan, Italy, and Austria’ had cooperated to amass a naval and military force to subdue the violence that had sprawled out of control (Naval History and Heritage Command, 2015).

While Western states and Japan perceived armed intervention as a necessary cooperative act to bring an end to sporadic and unchecked sanguinary, years down the line the military ethos and overall propaganda line of China is predicated on military strength to fend off ‘would-be subjugators’ (Kaufman, 2011, p.3). States that are on the receiving end of violent cooperation may choose to form allegiances to make sure that collective intervention against them remains in history books. Cooperation does not always produce benevolent or virtuous outcomes. Indeed, cooperation can be a tool of oppression.

In another example, cooperation by South American states during Operation Condor led to the abduction, rendition and assassination of ‘thousands upon thousands of murders... from 1973 to 1980’ (Dinges, 2005, p.1; National Security Archive (US), 2015). In this example a term analogous to cooperation, such as collective security, was aggrandised to enable South American ‘security services to join forces to track down “terrorists” of all nationalities, wherever they resided’ (Dinges, 2005, p.4). Collective security is defined

as ‘[a] security regime agreed to by the great powers that set rules for keeping peace, guided by the principle that an act of aggression by any state will be met by a collective response from the rest’ (Blanton and Kegley, 2017, p.31). At the time, Chilean dictator, General Pinochet, who created Operation Condor along with Uruguay, Paraguay, Bolivia, Argentina (and later Brazil) saw the fate of each Condor nation’s battle with insurgent forces and protestors as entangled among each other. Military leaders found it necessary to cooperate to bring about the ‘eradication’ of ideological enemies throughout Latin America before the rot spread and posed an overwhelming revolutionary risk to all authoritarian regimes on the continent (Dinges, 2005, p.3).

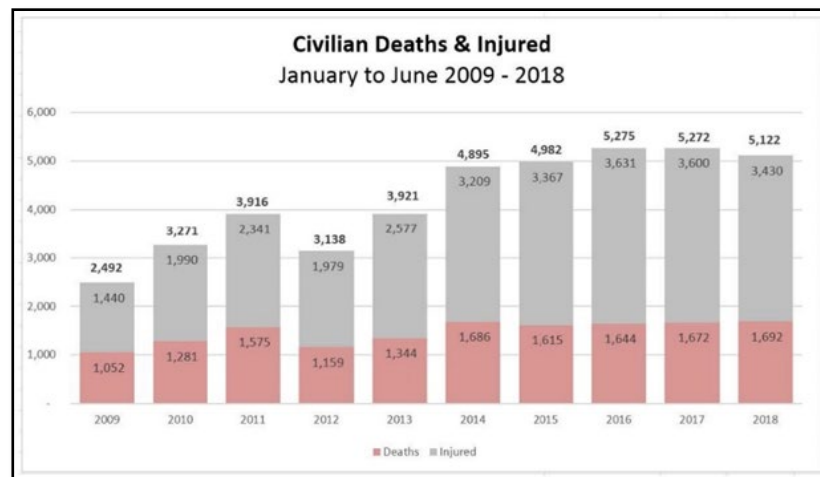


Figure 7: UNAMA, 2018

Furthermore, an identical concept used by NATO is collective defence (2018[a]). According to NATO, ‘[c]ollective defence means that an attack against one Ally is considered as an attack against all [a]llies’ (2018[a]). NATO’s collective defence is referred to as ‘[a]rticle 5 of the Washington Treaty’ (2018[a]).

Ironically, collective security to some extent grows out of liberal institutional values and refers to a coalition of important actors within the international arena that endeavour to suppress aggression by rogue states (Pevehouse and Goldstein, 2013, p.78). However, after the 9/11 terrorist attack in New York, NATO was quick to trigger article 5 that subsequently led to the US and NATO invasion of Afghanistan. Unfortunately, according to the United Nations Assistance Mission in Afghanistan (UNAMA) ‘[c]overing the

period 1 January to 30 June 2018, findings include the killing of more civilians in the first six months of this year – 1,692 deaths – than at any comparable time over the last ten years since records have been kept’ (2018) (See Figure 7).

NATO’s near failed odyssey in Afghanistan has reminded the world that cooperation is not always benign, even if the initial intent on paper was. However, the nature of collective security goes beyond hard power warfare and disastrous life-threatening sanctions. As the frequency of nefarious Russian activity in cyberspace increases, the question as to whether NATO’s collective security should be endorsed with regards to cyber-attacks pushes the world closer to a dangerous precipice. NATO’s Secretary-General Jens Stoltenberg addressed this situation, stating that:

*In 2014, NATO leaders agreed that a cyber-attack could trigger Article 5 of our founding treaty. Where an attack on one Ally is treated as an attack on all Allies. Traditionally, an Article 5 attack would be with tanks, aircraft and soldiers. Now it can come in the form of a cyber-attack. Placing cyber at the very heart of what we do (NATO, 2018[b]).*

Information and intelligence will play a crucial role in shaping collective security and cooperation in the years to come. Pivoting back to the specific concept of cooperation, the field of intelligence is also increasingly relevant. As noted in the introduction, the Anglo orientated international cyber intelligence organisation of Five Eyes seeks to combine sophisticated intelligence measures and infiltrate the networks of foreign adversaries and allies. This is a crucial contemporary example of cyber intelligence cooperation.

---

## 2.7 Cyberspace

---

In the 21<sup>st</sup> century, cyberspace has played an integral role in both supporting and undermining the security of nations worldwide. Civilians and the nation-state have become inexorably bound to cyberspace due to the vast opportunities this domain provides for both groups to increase commerce, transmit news broadcasts, find entertainment, life partners, conduct computer network-based attacks, surveillance and propaganda campaigns. Cyberspace is not necessarily a physical domain. The existence of cyberspace is predicated ‘upon physical assets – power sources, cables, networks, data-

centres, as well as the people who operate and manage them' (Ministry of Defence, (UK) 2016, p.14). MI5's definition of cyberspace has highlighted that:

*Cyberspace' is the term used to describe the electronic medium of digital networks used to store, modify and communicate information. It includes the Internet but also other information systems that support businesses, infrastructure and services (MI5, n.d.[a]).*

MI5's definition is relevant to this thesis as it illuminates the aspect of modifying information which is an essential theme in Chapter 6, 7 and 8. Within cyberspace, information can be sent from one side of the world to another in a short space of time. Moreover, platforms such as Google and YouTube, allow people to search for information and videos that have been uploaded by amateurs, politicians, chefs, news stations, scientists and various other groups or job occupations in society. As a result, the amount of information available has increased exponentially ushering in the dawn of the information age, within cyberspace. Although it is worth noting that the digitisation of information has significantly contributed to the information age, non-computer based information such as books has also had a role to play.

In the modern information age, the means to communicate through smartphones, laptops, and computers may be physical, but cyberspace is the domain in which a significant amount of information ends up for the world to see. Platforms such as Twitter, Instagram and YouTube allow people to interact with billions of people worldwide at a simple click of a button. In cyberspace, billions of people reside without physical connection as opposed to hundreds of people in a small village holding on (separately) to a newspaper. Theoretically, those who preside over others or have access to important information have a new stirring pot to add an assortment of propaganda. Also, the power to rule over emotions through grand decrees is no longer exclusively in the hands of traditional rulers. Non-state groups can embellish in any form of truthful or vacuous information for propaganda purposes. Alex Jones, for example, was one of the most-watched social media conspiracy theorists in the world who used his online platform to claim that Hillary Clinton and President Obama were demons from Hell (Stack, 2016). No matter how offensive, such comments may be, the power to inform and deceive is being adopted by non-state groups in cyberspace.



---

## 2.8 Intelligence

---

Intelligence, irrespective of how it is collected has played an integral role in national security both during times of peace and warfare. Succinctly put, Intelligence is ‘information relevant to decision-making’ (FBI, n.d.[a]). However, this definition does not suffice. A slightly more expansive definition provided by Martin Bimfort captures various aspects concerning the target of intelligence collection and how this relates to foreign policy.

Accordingly:

*Intelligence is the collecting and processing of that information about foreign countries and their agents which is needed by a government for its foreign policy and for national security, the conduct of non-attributable activities abroad to facilitate the implementation of foreign policy, and the protection of both process and product, as well as persons and organizations concerned with these, against unauthorized disclosure (Bimfort, 2011).*

I concur with Bimfort’s definition attempt, but, intelligence collection is too diverse to be viewed in a homogenous manner. In fact, there are various forms of intelligence, such as Signals intelligence, and Electronic Intelligence (ELINT) Human Intelligence (HUMINT) and others. Simply put, ‘Human intelligence...is information acquired by human sources through clandestine collection’ (CIA, 2016[a]).

SIGINT, on the other hand, opens up intelligence collection to a wider target audience. As summarised by the NSA, ‘SIGINT is intelligence derived from electronic signals and systems used by foreign targets, such as communications systems, radars, and weapons systems’ (n.d.[a]). The key to understanding the importance of SIGINT is that it ‘provides a vital window... into foreign adversaries’ capabilities, actions, and intentions’ (NSA, n.d.[a]). For example, during WW2 Secret ‘Ultra’ intercepts ‘had provided Bletchley Park with an intimate picture of the build-up of German forces in the east, prior to their attack on the Soviet Union’ (Aldrich, 2011, p.32).

Additionally, ELINT is a sub-branch of SIGINT. In the view of Charles Kroger ‘ELINT is the detection and analysis of radiations from foreign electronic devices for the purpose of extracting information of value to intelligence’ (2011). Moreover, according to the 1955 US National Security Council (NSC) Intelligence Directive No 17, ELINT is defined as ‘the collection (observation and recording), and the technical processing for later intelligence purposes, of information on foreign, non-communications, electromagnetic radiations emanating from other than atomic detonation sources’ (Office of the Historian, 1955). A key difference in definitions is the fact that ELINT is focussed on non-communicative devices. Typically ELINT would pick up ‘radars and other weapons systems’ such as a missile guidance device (Kroger, 2011; CIA, 2013[a]). Historically, ELINT endeavours such as Grab and Poppy were of great use to America’s efforts to determine the size of the Soviet Union’s arsenal during the Cold War (McDonald and Moreno, 2005, p.21; NRO, 2005, p.1).

---

## 2.9 Cybersecurity

---

Cognisant of the raft of issues within cyberspace, government agencies and private vendors are tasked with providing security to the state, companies and civilians. Recently the Canadian government have defined cybersecurity as ‘the protection of digital information and the infrastructure on which it resides. Cybersecurity addresses the challenges and threats of cyberspace to secure the benefits and opportunities of digital life’ (Department of Public Safety and Emergency (Canada), 2018). In a similar attempt, cybersecurity is defined as ‘the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks’ (Kaspersky, 2019[a]).

Essentially, the protection of devices that help to formulate or store information in cyberspace is a vital issue that will be highlighted throughout this thesis. Both state and non-state actors establish security measures. Cyber initiatives promulgated by the UK have been responsible for identifying and blocking millions of attacks that are aimed at the UK (NCSC, 2018[b]). Furthermore, companies such as FireEye and Kaspersky are prominent cyber vendors that provide endpoint security. Also, organisations such as IBM have created an X – Force Threat Intelligence unit, which:

*[A]nalyze data from hundreds of millions of protected endpoints and servers, along with data derived from non-customer assets such as spam sensors and honeynets. X-Force also runs spam traps around the world and monitors tens of millions of spam and phishing attacks daily. It analyzes billions of web pages and images to detect fraudulent activity and brand abuse (IBM, 2018, p.3).*

Also, non-state bodies such as the International Organization of Standards (ISO) contribute to cybersecurity by helping to set international encryption standards (Menn, 2017). Conversely, at times, Intergovernmental organisations (IGO) and Non-Governmental Organisations (NGO) are nothing more than fodder for powerful states. Thanks to Snowden, the world is now aware that the NSA attempted to pressure international organisations into adopting flawed encryption standards in order to penetrate the networks of other nations (EFF, 2013[a], p.1-2; Menn, 2017). Cybersecurity is thus a sensitive concept that needs to be addressed, concerning the rapidly evolving cyber environment.

---

## 2.10 Cyber Espionage and Cyber-Attacks

---

Terms analogous to surveillance such as espionage and cyber espionage also need to be defined to provide a broader context for this thesis. According to MI5:

*Espionage is the process of obtaining information that is not normally publicly available, using human sources (agents) or technical means (like hacking into computer systems). It may also involve seeking to influence decision-makers and opinion-formers to benefit the interests of a foreign power (MI5, n.d.[b]).*

Cyber espionage is thus the ‘extension of traditional espionage’ in cyberspace (MI5, n.d.[a]). As acknowledged by MI5, ‘[e]spionage activity is also carried out in cyberspace. Foreign intelligence services increasingly use the Internet and cyber techniques to conduct espionage against UK interests’ (n.d.[c]). Cyber espionage is a desirable option for state and non-state groups as it can be conducted from a distance with ‘relatively little risk’ to those that are involved (MI5, n.d.[a]). States often engage in Computer Network

Exploration (CNE) to penetrate and study networks or possibly even manipulate network infrastructure. To note, CNE and a similar term, EI, are somewhat interchangeable terms (MI5, n.d.[d]). Taken from a leaked GCHQ slide, '[c]omputer [and] Network Exploitation delivers to GCHQ data of intelligence value by remote access to computers, computer networks and telecom networks without the knowledge or consent of their owners and users' (The Courage Foundation, n.d., p.2). In terms of EI, MI5 has asserted the view that:

*Equipment interference, also known as computer network exploitation (CNE), allows MI5 to interfere with electronic "equipment". This includes computers, computer media (such as CDs or USB sticks) and smartphones for the purpose of obtaining communications or other information. Equipment interference encompasses a range of activity, from remote access to computers and other electronic equipment to covertly downloading the contents of a mobile phone or storage media during a search (MI5, n.d.[d]).*

Computer Network Attacks (CNA) is also a form of infiltration; however, the perpetrator is specifically trying to disrupt its targets ability to function effectively. In the view of MI5, CNA is based on the use of 'software... to disrupt and damage cyberinfrastructure. This can range from taking a website offline to manipulating industrial process command and control systems. Such activity is known as Computer Network Attack (CNA)' (n.d.[a]) (see chapter 7). Moreover, the Canadian government's definition of a cyber-attack points out the different intentions of an attack. According to the Canadian Government, a cyber-attack is an:

*Attack that involves the unauthorised use, manipulation, interruption or destruction of, or access to, via electronic means, electronic information or the electronic devices or computer systems and networks used to process, transmit or store that information (Department of Public Safety and Emergency (Canada), 2018).*

To be clear, EI and hacking will be used interchangeably. CNA as a term will seldom be used. At this juncture, it is vital to highlight that CNA, CNE or EI are all measures taken to help control the information environment. Information superiority is a term used within Britain's military discourse to express the desire to control the information space to benefit the British armed forces, whether it be psychological, e.g. public opinion or

technological, e.g. take over a nation's radar system. According to the Ministry of Defence (UK) 'the competitive advantage gained through the continuous, directed and adaptive employment of relevant information principles, capabilities and behaviours' can be described as 'information superiority' (2013, p.10). Ultimately, the drive to master information can push states to engage in morally questionable acts.

Hactivism, on the other hand, is a form of civil disobedience within cyberspace that is predicated on undermining network security of other companies, citizens or governments, for social or political goals. To be precise, hacktivism can be defined as 'the emergence of popular political action, of the self-activity of groups of people, in cyberspace. It is a combination of grassroots political protest with computer hacking' (Jordan and Taylor, 2004, p.1). Non-state groups often illegally access the networks of companies and governments to steal information that is to be later released to the world. WikiLeaks, for example, uncovered sensitive footage from the US, which revealed American soldiers in helicopters shooting at Iraqi civilians in 2007 (McGreal, 2010).

In other instances, hacktivism or hacktivists can deface and impede the function of Internet websites of companies or governments in the form of Distributed Denial of Service attacks (DDoS) as a means of making a political statement. Of late Kaspersky have highlighted that a 'DDoS attack will send multiple requests to the attacked web resource – with the aim of exceeding the website's capacity to handle multiple requests... and prevent the website from functioning correctly' (Kaspersky, 2019[b]). On the other hand, it is vital to note that governments are capable of using DDoS attacks as a tactic to take down targets. Back in 2011, GCHQ targeted the hacktivist group Anonymous with a DDoS attack called ROLLING THUNDER, demonstrating that intelligence services are adaptable and willing to use techniques usually associated with hacktivism (NBC NEWS, 2014[a]).

---

## 2.11 Surveillance and Mass Surveillance

---

Surveillance has come to be a topical issue in the 20th and 21st century, although it is imperative to highlight David Lyon's assertion that '[s]urveillance is not new' (1994, p.22). Stretching back to the Old Testament, after the death of Moses Joseph sent spies into Canaan to 'secretly explore the land of Canaan, especially the city of Jericho' in order to assess the strength of the inhabitants (Joshua 2: 1). Sometime after this form of HUMINT was relayed back to Joseph, his men 'killed everyone in the city, men and women, young and old', bringing victory to the Jews of the Old Testament at the expense of the people of Jericho (Joshua 6: 21). Centuries later, America began forming its first field intelligence unit that used extensive intelligence work to identify and pacify the population of the Philippines during its colonial conquest and counterinsurgency campaigns (McCoy, 2015, p.4).

In contemporary times, surveillance is still used to help facilitate the conquest or subjugation of other people. As highlighted by Martin Innes 'in late-modernity, the conducting of surveillance has infiltrated a variety of public and private institutions, via a panoply of techniques and technologies' (2003, pp.112). In other words, modern surveillance is not only wielded by powerful imperial nations in a top-down manner. Typically, surveillance is associated with an element of control by powerful states against civilians who do not have a specific amount of control over their personal information or how they're observed. Innes argued that '[s]urveillance is a mode of social control that has undergone rapid change and development in late-modern societies' (2003, p.130). Before this rapid expansion, surveillance was generally viewed in a positional or hierarchical context associated with Jeremy Bentham's concept of the Panopticon (Foucault, 1991, p.201).

As such, '[t]he types of surveillance accentuated in the panoptic model typically involve the monitoring of people who reside at a lower point in the social hierarchy' (Haggerty, 2006[b], p.29). Postulated by Bentham and reinvigorated by Foucault, the Panopticon structure consists of a guard within a prison structure watching inmates who are unable to verify whether the guard is watching them due to his confined position in a cell and the guard's hierarchical position (1991, p.200). The element of risk exercises control over the

inmate due to the hierarchical position and the inmate's inability to locate the exact position of the guard (Foucault, 1991, p.202). Additionally, as will be discussed in Chapter 7, modern surveillance has evolved to the extent that previous hierarchical assertions concerning surveillance are potentially obsolete or at least ill-suited to new domains since non-state groups and citizens can monitor those in power. (Haggerty, 2006[b], p.23).

Cognisant of the fact that this thesis revolves around surveillance in cyberspace, a definition that is associated with the use of the Internet to monitor people is required. According to Lyon, 'electronic surveillance has to do with the ways that computer databases are used to store and process personal information on different kinds of populations' (1994, p.8). Lacking in the emphasis of control and influence, an additional definition is required. As described by Lyon, surveillance is 'any collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been garnered' (2012, p.2). This definition is ideal since it encompasses both online and offline aspects to surveillance in conjunction with the aspect of control and influence.

Moreover, the Snowden leaks have reinvigorated the term mass surveillance and have brought greater scrutiny to the relationship between governments and their citizens (Bakir, 2015[b], p.12-13). For instance, the Snowden revelations highlighted America's infamous PRISM program, which indicated that the NSA was able to obtain information from telecommunications companies concerning their clients (Masco, 2017, p.394-395). Furthermore, the UK's Tempora program suggested that British intelligence services were able to intercept huge swathes of Internet traffic through the tapping of underwater fibre-optic cables (Fidler, 2015, p.200).

Another GCHQ project titled Karma Police was able to identify 'which websites your target visits, and when/where those visits occurred... who visits suspicious websites, and when/where those visits occurred... Which IP address and web browser were being used by your target when they visited a website' (The Intercept, 2015[b], p.2). Also, similar revelations showed that GCHQ's Optic Nerve program allowed them to hack into and access 'Yahoo! webcam chats' (Elsayed-Ali, 2015). Lastly, it is vital not to overlook

GCHQ's ambitions of 'Target Discovery at Population Scale' (The Intercept, 2015[c], p.8).

**Target Discovery at Population Scale**

- We are describing a *target discovery* technique based on *known target communications behaviour* applied to *population scale bulk unselected* events
- *target discovery* – discover *unknown* targets
- *known target communications behaviour* – modus operandi (MO)
- *population scale* – *all* the events we have for a country
- *unselected events* - not seeded on targets

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on [REDACTED]

ICT RESEARCH      UK TOP SECRET STRAP1 5EYES      NEXT GENERATION events

Figure 8: The Intercept, 2015[c], p.8

Western intelligence services have been learning how to monitor and intercept vast amounts of data. As a result, surveillance as a concept was elevated to a relatively new level which put the mass in mass surveillance. Post Snowden, the British Government has openly pushed for the ability to hack devices on an international scale. To begin with, the British government's exoneration of EI as its right to hack large swathes of foreign networks serves as a starting point to highlight the endemic anarchic scenario that exists in cyberspace (House of Commons, 2015[a], p.1). Unbeknownst to some, EI is nothing new to the UK government. The Intelligence Services Act states that GCHQ's functions 'shall be... to monitor or interfere with electromagnetic, acoustic and other emissions and any equipment producing such emissions and to obtain and provide information derived from or related to such emissions or equipment and from encrypted material' (Intelligence Services Act, 1994, p.4).

In contemporary times, the UK government have made the case that 'equipment interference... is the power to obtain a variety of data from equipment' (House of Commons, 2015[b], p.1). To be precise, equipment encompasses, 'computers or computer-like devices such as tablets, smartphones, cables, wires and static storage devices' (House of Commons, 2015[b], p.1). EI is used by 'security and intelligence



agencies, armed forces and law enforcement agencies, to interfere with equipment for the purpose of obtaining electronic data from the equipment' (House of Commons, 2015[b], p.1).

As stated by MI5 '[e]quipment interference, also known as CNE, allows MI5 to interfere with electronic "equipment"' to gain vital intelligence concerning national security (2018[d]). Moreover, with regards to GCHQ, it was made clear in a hearing by the Investigatory Powers Tribunal that it is possible that CNE/EI will be used and will involve:

*[T]he obtaining of information from a particular device, server or network... the creation, modification or deletion of information on a device, server or network; the carrying out of intrusive surveillance...the use of CNE to weaken software or hardware at its source, prior to its deployment to users (Anderson, 2016, p.42-43).*

Essentially, Britain's intelligence services have the legal and technological capacity to hack into networks at their discretion for the sake of national security. There are two types of EI. TEI and Bulk EI. Targeted interception is used when there is an obvious target that is using a specific device. Paradoxically the term TEI at times is not accurate. The British government have conceded to the fact that '[i]t is entirely possible for a targeted 'thematic' EI warrant to cover a large geographic area or involve the collection of a large volume of data' (House of Commons, 2015[d], p.31). Therefore, even when British intelligence services are trying to limit the degree of intrusion, innocent citizens that may have nothing to do with an investigation are at risk of having their devices hacked.

On the other hand, Bulk EI is used when a known threat exists, but intelligence services do not know precisely where it is or the specific device that needs to be infiltrated. Consequently, Bulk EI requires British intelligence to hack into a significant amount of devices across a large geographical area. To be more specific, bulk EI is used when, for example, 'little is known about the individual members of the terrorist cell. No technical details are known about their communications or the devices they are using' (House of Commons, 2015[d], p.32).

As noted by the UK government's fact sheet on bulk EI, '[b]ulk EI facilitates target discovery, it helps to join up the dots between fragments of information that may be of intelligence interest' (House of Commons, 2015[a], p.1). This is the equivalent of throwing a large fishnet out in the sea rather than throwing a spear at a known fish that one can see. Bulk EI is foreign-focused. However, the distinction between bulk EI and TEI is a cause for concern for foreign nations due to the scale at which devices and networks can be hacked or disrupted.

A British government Parliamentary intelligence committee report on the investigatory powers bill raised issues with the alleged distinction between targeted and bulk EI. The report stressed that '[d]espite the name, a Targeted EI warrant is not limited to an individual piece of equipment, but can relate to all equipment where there is a common link between multiple people, locations or organisations' (Parliament. House of Commons, 2016, p. 8[a]). Again, it is crucial to accentuate the possibility that innocent citizens can have their devices hacked into by a foreign (British) intelligence service. To some degree, cyber stability is, therefore pegged to the inability of intelligence services to curtail the number of devices that can be hacked, in order to find the actual target.

In evidence presented to the Intelligence and Security Committee of Parliament the Director of GCHQ suggested that, hypothetically, a 'Targeted EI warrant could cover a target as broad as an entire hostile foreign intelligence service' (Parliament. House of Commons, 2016, p. 8[a]). Members went on to state that it 'is therefore unclear what a 'Bulk' EI warrant is intended to cover, and how it differs from a 'Targeted' EI warrant (Parliament. House of Commons, 2016, p. 8[a]). GCHQ emphasised the above point by admitting that the '*dividing line between a large-scale targeted EI and bulk is not a specific one* (Parliament. House of Commons, 2016, p. 9[a]).

In other words, Britain's intelligence services can theoretically or quite literally hack an untold amount of devices throughout various parts of the world despite what any other government may think about their citizen's devices being undermined. Considering the fact that the British government has authorised EI since at least 1994, the question must be asked; what government or international system can stop Britain from doing this? By stop, I do not mean in the sense of bolstering endpoint cybersecurity. I am referring to international agreements, norms and most importantly, international (governing) centres

of power such as the EU, NATO, the UN, AU or even the Shanghai Corporation to step in and restrain the UK. Without some form of restraint, the UN's desired goal of cyber stability will cease to be of any genuine relevance. The answer to the most recent question is that no one can. Hacking is a part of the security apparatus of a state to protect itself from real and imaginary fears of current and future hostile enemies. Moral reasoning to extenuate EI is based on a pretext of outmanoeuvring nefarious threats such as terrorists and hostile states (House of Commons, 2015[a], p.1).

Further issues exist within the dichotomy of domestic and foreign targets of EI. According to the British government, a great amount of emphasis is given to the fact that UK intelligence services focus a lot of their intrusive capabilities towards foreign targets. As such 'bulk interception warrant' and 'a bulk EI warrant must be foreign-focused' (House of Commons, 2015[d], p.30). In reality, this distinction is supposed to appease UK citizens and dissociate fears of an Orwellian state with profound domestic surveillance powers.

At this stage, the difference between people who matter and 'unpeople' becomes clear (Chomsky's Philosophy, 2015). Put eloquently in a speech made by Chomsky 'people are those who count. Un-people are those who are not human, you can do anything you can do anything to them' (Chomsky's Philosophy, 2015).<sup>6</sup> In this context, unpeople are non-British citizens, particularly those outside of the Five Eyes Anglosphere. The UN is designed to protect all citizens. However, with regards to surveillance, nations tend to offer more protection to domestic citizens than people from foreign countries.

Conversely, unlike Hollywood films such as the Independence Day where US superior hacking technology saved the world, or James Bond films where the Brits always win, other nations have intrusive technology. Ironically, Britain sells such software abroad. Foreign powers may also feel insecure and will want to keep tabs on Western endeavours. Perhaps data on British citizens is up for grabs by rogue or even friendly nations that just so happen to perceive everyone outside of their borders as 'Unpeople' (Chomsky's Philosophy, 2015). According to the BBC's investigation on the surveillance industry, Britain's 'defence giant BAE Systems has made large-scale sales across the Middle East

---

<sup>6</sup> Un-people is a term coined by George Orwell but highlighted by Noam Chomsky.

of sophisticated surveillance technology’ (2017[a]). Unsurprisingly, some of the technology sold included ‘decryption software which could be used against the UK and its allies’ (BBC, 2017[a]). Professor Ross Anderson gave a scenario on such occurrences stating that:

*An Arab country wants to buy cryptanalysis equipment supposedly for its own law enforcement. They have embassies in London, Washington, Paris and Berlin. What's to stop them putting bulk surveillance equipment in our cities and then using the cryptanalysis equipment to decipher all the mobile phone calls they hear?* (Anderson, 2017, cited in BBC, 2017[a]).

Due to the cover of cyberspace, the UK has no guarantees that friendly nations will not aim cyberweapons at her. Cognisant of the extensive information presented above concerning EI and its ramifications, mass surveillance needs to be defined in context to provide a clear conceptual watershed from monitoring. Sarah Logan’s work on mass surveillance focused on post 9/11 anxiety in the US which spurred the drive to collect vast swathes of information (2017, p.1-2). Under the direction of General Keith Alexander, the NSA adopted an ethos of collecting ‘the whole haystack’ – meaning an almost limitless range of metadata, which the agency stores for five years, possibly longer’ (Logan, 2017, p.2). In this context, Logan has asserted the view that:

*Mass surveillance differs from other forms of surveillance because it relies on the collection and manipulation of massive data sets. A massive technological system, it is conceived of and used as a data set rather than individual data points – as ‘the whole haystack’ rather than, for example, the single street surveilled by a street camera* (Logan, 2017, p.2).

From this perspective, people that are of no intelligence interest may be victims of mass surveillance merely because they exist within the matrix of information available for the taking. Albeit somewhat awkwardly defined, the definition that I adhere to was construed by Lyon who stated that by ‘definition, mass surveillance means that anyone and everyone can be caught in the surveillance net and the larger the scale of surveillance, the more likely it is that false positives will emerge in the quest for ‘persons of interest’ (2015, p.142). Before moving forward, an issue exists between the association of mass surveillance and global surveillance. Mass surveillance could simply mean mass

surveillance on a domestic front. In contrast, global surveillance could mean, for example, the NSA's 'ability to sweep up billions of messages worldwide and monitor specific international leaders' (McCoy, 2015, p.14).

At times both mass surveillance and global surveillance can be perceived as interchangeable terms, which may confuse readers. For the sake of clarity, this thesis will adhere to Lyon's depiction of mass surveillance which is circumstantial, that is, the context of the matter at hand may refer to national or international levels of mass surveillance (Lyon, 2015, p.142). Generally speaking, considering the Snowden leaks, mass surveillance will typically apply to large scale international surveillance activities by both state and non-state actors.

---

## 2.12 Propaganda

---

Much like the phenomenon of surveillance, propaganda is 'is thousands of years old' (Welch, 2013, p.2). The rise of propaganda in the 20<sup>th</sup> century appeared to be correlational with the sophistication of mass media which provided propagandists with 'fertile ground' to spread falsehoods domestically and internationally (Welch, 2013, p.2). Early 20<sup>th</sup> century technological advancements saw newspapers, radio broadcasting and the cinema help the state to communicate fundamental narratives to domestic and foreign citizens (Haste, 1977, p.3; Finch, 2000, p.371; Fox, n.d.). Cyberspace has provided yet another medium for propagandists to influence the masses (BBC, 2017[b]). Before providing context for this new situation, it is vital to define propaganda. Thankfully, examples and definitions of propaganda are not hard to come by. There is no one universally accepted definition of propaganda that is endorsed by all academics. In fact, according to John Martin, 'there is no consensus either among the practitioners or among the theoreticians as to what constitutes propaganda' (Martin, 1971, p.62).

Martin defined propaganda as 'a persuasive communicative act of a government directed at a foreign audience' (1971, p.62). However, Chapter 7 is focused on a tainted leaks campaign initiated by a Russian state-linked non-state group, although it is unclear if they received direction from the Russian government. Therefore, this truncated and somewhat old definition may appear as obsolete. Ironically, Harold Lasswell's definition and

explanation of propaganda, which came into existence almost a century ago, resonates well with the modern period in terms of its functionality. Lasswell's attempt at defining and explaining propaganda allows for one to conceptually pivot and embrace the endless means and forms propaganda can manifest itself in. Lasswell has defined propaganda as the 'management of collective attitudes by the manipulation of significant symbols' (1927, p.627). Reflexively, readers might assume that symbols represent images such as a Swastika or an Adidas logo.

However, Lasswell expands on the meaning of symbols in stating that 'significant symbols are paraphernalia employed in expressing... attitudes...The form in which the significant symbols are embodied to reach the public may be spoken, written, pictorial, or musical, and the number of stimulus carriers is infinite' (1927, p.631). YouTube, Facebook and Twitter are cyberspace mediums identified by GCHQ as places to launch their propaganda campaigns (Dhami, 2011, cited in *The Intercept*, 2015[a], p.2). Lasswell's comprehensive explanation and definition of propaganda match the current litany of mediums used to transmit propaganda online.

Moreover, there is one key element from this package definition of propaganda that has not been emphasised. Propaganda usually plays to the irrational, reactionary faculty of humankind. In the view of Ernest Beaglehole propaganda can be defined as 'the process whereby public opinion is formed and controlled by appeal to the irrational side of man's nature in such a way that it is usually favourable to the interests of those directing the propaganda' (1928, p.96). For example, US President Donald Trump was publicly scrutinised for airing a racist TV ad during the US midterm elections. This particular ad portrayed Latin Americans as a threat to national security when President Trump pledged to move the military to block the entry of Latin American migrants from crossing the US border (Collinson, 2018).

Conversely, this was a well-timed propaganda ploy that played into the irrational aspect of President Trump's most loyal supporters (Collinson, 2018; Greenberg, 2018). Accordingly, irrationality is a crucial aspect of propaganda. In light of this assertion, it is vital to point out that propaganda varies in terms of its authenticity and the source. Propaganda is often graded by colour to denote the legitimacy of the source and content. According to Garth Jowett and Victoria O'Donnell white propaganda:

*[C]omes from a source that is identified correctly, and the information in the message tends to be accurate... Although what listeners hear is reasonably close to the truth, it is presented in a manner that attempts to convince the audience that the sender is the “good guy” with the best ideas and political ideology (Jowett and O’Donnel, 2011, p.17).*

The most controversial chapter (chapter 5) in this thesis is predicated on the US 2016 presidential election and the subsequent ontological tremors experienced by the USG. This particular chapter depicts white propaganda, albeit information was stolen from the DNC. Although, it is essential to highlight that the release of unsavoury information concerning the DNC was flanked by black propaganda in the form of trolls and malicious websites purporting to be Americans but were Russian made. Also, it is vital to note that governments and their militaries use Psychological Operations (PSYOP) to influence foreign target audiences, predominantly in war zones or regions of value, to construe narratives that are congruent with government and military policy of an occupying force.

PSYOP’s have been defined by NATO as the ‘planned activities using methods of communication and other means directed at approved audiences in order to influence perceptions, attitudes and behaviour, affecting the achievement of political and military objectives’ (Ministry of Defence, 2015, p.18). PSYOP products typical consist of radio communication, loudspeakers and leaflets. The US armed forces used PYOP’s to try and shape the information environment during its military occupation of Iraq and Afghanistan (Munoz, 2012, p.29). To an Iraqi or Afghan civilian that has been subject to US PSYOP’s, the concept of PSYOP’s may be viewed as a mischievous form of propaganda that has a verifiable source but does not contain the perspective of those that have been occupied by a hostile foreign power.

In the case of grey propaganda, it lies ‘somewhere between white and black propaganda. The source may or may not be correctly identified, and the accuracy of the information is uncertain’ (Jowett and O’Donnel, 2011, p.20). This particular definition resonates much with Chapter 8 that is predicated on the usage of covert psychological warfare. In this example, British PR firm Bell Pottinger edited existing terrorist propaganda before being released to the public under the guise of a legitimate local news source. Grey propaganda

is crucial to the analysis of my work, as the ambiguous source and content in some cases can leave people in a state of confusion over whether they can trust information or not.

Finally, information that is classed as black propaganda ‘when the source is concealed or credited to a false authority and spreads lies, fabrications, and deceptions. Black propaganda is the “big lie” including all types of creative deceit’ (Jowett and O’Donnell, 2011, p.18). This explanation will be used to help dissect Chapter 6 in order to evaluate the FBI’s cyber campaign to catch terrorists. Cognisant of the evolving nature of propaganda campaigns and the subjective nature of interpreting truths, placing a form of propaganda into a single category is relatively difficult. Nonetheless, this thesis revolves around the dissemination of white grey and black propaganda, albeit predominantly geared towards black propaganda. A standout definition of propaganda that I will adhere to has been construed by Welch who defined propaganda as ‘the deliberate attempt to influence the public opinions of an audience, through the transmission of ideas and values, for a specific persuasive purpose that has been consciously thought out and designed to serve the self-interest of the propagandist’ (2013, p.2).

---

## **2.13 The Sham Universe and the Democratic Proselytisation of Terrorism**

---

It is necessary to highlight the meaning and context of the phrase sham universe. French Philosopher Jacques Ellul used the term in his influential book *The Technological Society*. Ellul used the term sham universe in the context of highlighting the ramifications of modernised propaganda engulfing society. Accordingly, a ‘consequence of technical propaganda manipulations is the creation of an abstract universe, representing a complete reconstruction of reality in the minds of its citizen’ (Ellul, 1965, p.371). Ellul was referring to the ability of propaganda and the propagandist to inculcate society so much that individuals accept this new mirage or picture that has been formed. Words, symbols and images communicated online and offline can construe a completely erroneous or partially false mirage ‘which may not reflect reality but which are truer than reality’ (Ellul, 1965, p.371).



Consequently, a sham universe resembles an environment of ‘hallucinations’ as opposed to reality in which people are led and directed to the ends of the propagandist (Ellul, 1965, p.372). As such, a sham universe represents the alteration of reality due to the potency and far reach of modern propaganda. For example, the fake mob that was engineered by the British intelligence and the CIA helped to topple Mosaddeq’s government in Iran, appeared to some as a genuine consensus for revolt (National Security Archive (US), 2013). Little did they know this ploy was part of a sham reality being engineered by foreign nations.

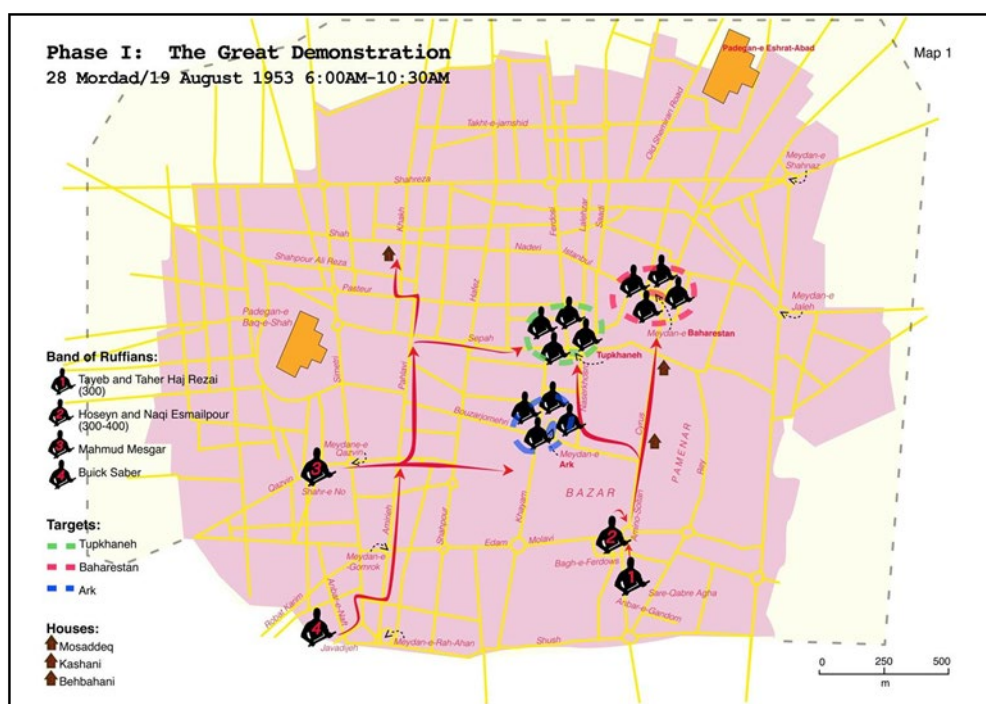


Figure 9: National Security Archive (US), 2013. This map shows the where paid protestors were sent in Iran to help facilitate the coup in 1953.

Ellul went on to state that this pretence aims to ‘form rather than to inform...[t]his kind of thing represents the first step toward a sham universe. It is also indicative of an important element in today's psychology, the disappearance of reality in a world of hallucinations’ (1965, p.371-372). In short, the sham universe is a constructed reality designed to influence a large portion of people. People are thus led to believe that a sham is real when, in fact, they are victims of an eloquently crafted ruse. As will be explained further in Chapter 6, the FBI appears to have prepared a sham universe for terrorist sympathisers,

which accelerated the transition from supporting jihad online to making concrete and active steps to travel to Syria and fight.

Furthermore, it is vital to outline the term democratic proselytisation of non-state terror. This is a term I have coined to present the irony of democratic attempts to preserve democracy while directly or indirectly exonerating propaganda that supports terrorism. Since the inception of DAESH, Western governments and academics have become fascinated with the potency of online propaganda (Edwards, 2015, p.12-13; Boyle, and Mower, 2018, p.205-206; Chatterjee, 2016, p.201-202; Home Office, 2018, p.11). Thousands of people from 110 countries have been attracted to DAESH, which has been attributed to propaganda videos in cyberspace that exonerate DAESH (BBC, 2017[c]).

Paradoxically, evidence provided by FBI agents under oath has revealed that the Bureau has done precisely what governments and think tanks have feared. That is, to encourage citizens to join a terrorist organisation and proselytise the act of terrorism. The FBI's pledged to buy bus tickets, introduce mentors, guarantee physical training and a string of other incentives are what I refer to as jihadi carrots. To be clear, the democratic proselytisation of terror can be described as the encouragement of citizens or non-state actors to engage in terroristic activity by democratic nations and their intelligence services. The term democratic proselytisation of terrorism is thus meant to emphasise the fact that the so-called democratic leader of the free world, uses its intelligence services (the FBI) to purposefully target people online and encourage them to commit acts of terrorism (see chapter 6).

Although Bond movies and sensational conspiracies may have sexed up and exaggerated how cavalier British and American intelligence services operate, the FBI's proselytisation of terrorism seems to be a step too far. To be clear, although some of the FBI's messages were directed at individuals, I still class this as propaganda. Put eloquently by Ellul '[p]ropaganda tries to surround man by all possible routes, in the realm of feelings as well as ideas, by playing on his will or on his needs' (1973, p.11). Furthermore, the terrorist web page was put on the Internet. In theory, it was accessible for billions of people worldwide. Also, Ellul suggested that propaganda is an 'organized myth that tries to take hold of the entire person'; in this case, individuals targeted by the FBI (1973, p.11).

---

## 2.14 Risk

---

The term risk is a prominent feature of human history in the sense that people are ‘surrounded by risks... and always have been’ (Leiss and Chociolko, 1994, p.6). Beck suggested that risk ‘means the anticipation of catastrophe’ (2006, p.332). Having employed the word anticipation, risk is not necessarily a tangible physical feature of society despite how frequently used this word (risk) is. Instead, risk is capricious since it is ‘existent *and* non-existent’ (Beck, 2009, p.3). According to Pat Caplan’s summary of Beck’s book *Risk Society*, ‘[m]odern risks are typically invisible, located in the spheres of physics and chemistry’ (2000, p.3). However, some of Beck’s later work opened up the scope of Risk Society to digital risk and modern surveillance within cyberspace (2016, p.141).

---

## 2.15 Ontological (In) Security

---

OS is a central concept that underpins the theoretical orientation of this thesis. The conceptual derivative of the term OS is rooted in the field of psychology. This stance is reflected in the work of Ronald Laing, which explored and dissected schizophrenia:

*The term schizoid refers to an individual the totality of whose experience is split in two main ways: in the first place, there is a rent in his relation with his world and, in the second, there is a disruption of his relation with himself. Such a person is not able to experience himself 'together with' others or 'at home in' the world, but, on the contrary, he experiences himself in despairing aloneness and isolation (Laing, 1965, p.17).*

As a consequence of disruption, the self no longer consists within a sphere of tranquillity, thus leaving people exposed to what Laing referred to as a:

*[P]artial or almost complete absence of the assurances derived from an existential position of what I shall call primary ontological security: with anxieties and dangers that I shall suggest arise only in terms of primary ontological insecurity; and with the consequent attempts to deal with such anxieties and dangers (Laing, 1965, p.39).*

For the sake of clarity, it is essential to acknowledge the difference between (OS) and OIS. OS is a sense of continuity and security concerning the surrounding environment. In contrast, OIS is the feeling of anxiety or cognitive distress that arises when the perception of impending risk diminishes a person's ability to manage concerns effectively. In this aspect, OIS can occur due to the plethora of existential 'anxieties to which all human beings are potentially subject' (Giddens, 1990, p. 94). To be ontologically secure 'a person must learn to trust, or develop a generalised sense of trust, in the nature and stability of the social and structural environments they inhabit' (Hewitt, 2010, p.511). Such trust typically manifests in the form of 'unquestioned sense of self and of his or her place in the world in relation to other people and objects' (Hewitt, 2010, p.511).

According to Giddens '[a] sense of the reliability of persons and things, so central to the notion of trust, is basic to the feelings of ontological security' (1990, p. 92). That is, an individual is to some degree, immersed in a socio-spatial environment which is imbued with stimuli that can change the equilibrium between OS and OIS. This balance must be continuously altered and consciously or unconsciously monitored and reacted upon to distil a sense of OS from a tumultuous environment. Other scholars such as Robert Hawkins and Katherine Maurer, have defined OS as the 'psychological protection from the anxiety of uncertainty and risk provided by everyday social activities, continuity, the home place and the value of community' (2011, p.144). In this respect, OS is centred on the phenomenological notion of being in the world (Browning and Joenniemi, 2017, p.44).

Moreover, OS and OIS have been appropriated and used within the discipline of politics and IR (Combes, 2017, p.139; Rumelili and Çelik, 2017, p.280; Hawkins and Maurer, 2011, p.144-146; Kumar, 2018, p.8; Subotić, 2016, p.611). With regards to the field of IR, Brent Steele has pointed out that '[i]f ontological security theory in IR is indeed its own 'tribe', it is becoming a larger one, or at least one inviting enough that other tribes seem to be noting its presence' (2017, p.70). States also suffer from OIS. Jelena Subotić's research has assessed identity preservation and narrative change of Serbian politicians during its paradoxical acknowledgement of Kosovo, despite previous refusals to do so (2016, p.611). Moreover, it is crucial to point out that predictability or rehearsed roles concerning political adversaries is essential to the concept of OS. At times states prefer

to always be at risk with an adversary that they are familiar with than to experience new relations which will force the state to traverse a new linguistic and conceptual Rubicon that the nation is not used to (Mitzen, 2006, p.341). In this context, OIS is a fundamental concept that will be used throughout this thesis.

---

## 2.16 Tainted Leaks

---

Tainted leaks is a term used to describe a recent propaganda and surveillance campaign in which documents were stolen from Journalist David Satter by hacking group CyberBerkut and then edited before being released to the public online (Hulcoop et al., 2017). The purpose of tainted leaks is to sway and manipulate public opinion within a domestic or foreign nation. Hulcoop *and colleagues* uncovered a ‘larger phishing operation, with over 200 unique targets spanning 39 countries (including members of 28 governments)’ (Hulcoop et al., 2017). Targets of intrusion (hacking) varied in social status and came from different backgrounds. For example, the ‘former Russian Prime Minister, members of cabinets from Europe and Eurasia, ambassadors, high ranking military officers, CEOs of energy companies, and members of civil society’ were targets of CyberBerkut’s phishing campaigns (Hulcoop et al., 2017).

Moreover, the intelligentsia were also targets of tainted leaks. A breakdown of statistics from Hulcoop and colleagues has demonstrated that the ‘second largest set (21%) are members of civil society including academics, activists, journalists, and representatives of non-governmental organizations’ (Hulcoop et al., 2017). To note, this indeed demonstrates the vast reach and lengths hackers are willing to go to in order to obtain the appropriate amount of information to launch propaganda campaigns. Tainted leaks as a concept is central to Chapter 7. Tainted leaks will be used in conjunction with Lippmann’s term the phantom public to assess the effects of propaganda and the extent to which the modern citizen is capable of dealing with the constant threat of false information.

---

## Chapter 3: History and Context of Propaganda and Surveillance 20<sup>th</sup> Century Surveillance

---

Undoubtedly, the history of surveillance operations between Western nations and their adversaries is extensive in detail. Over time, surveillance has become a crucial tool for Western governments to assist in managing empires, spheres of influence and global flashpoints. To fulfil such demands, the manner in which countries conduct surveillance operations has fluctuated between HUMINT, ELINT, SIGINT and other means of intelligence gathering. This chapter sets out to highlight key moments in British and American intelligence operations throughout the 20<sup>th</sup> and 21<sup>st</sup> century. Albeit, this is an extremely narrow scope; the depth and reach of US and British intelligence operations means that various regions of the world have been affected.

Furthermore, this chapter aims to highlight liberal institutional attempts in the 21<sup>st</sup> century to bring surveillance operations to a halt. In particular, the DGC and its theoretical roots will be explored. After presenting the case of a DGC, I will juxtapose this with modern examples of Realist self-help behaviour that manifests itself as surveillance via exploiting networks and undermining encryption standards. Demonstrating the circumstances in which liberal institutional endeavours drastically fail to bring an end to international surveillance campaigns is crucial to understanding the potency of Realist impulses that states experience which undermines global peace. In doing so, the modern context of propaganda and surveillance will be presented as a means of demonstrating how and why cyberspace is inexorably bound to elements of the Realist school of thought such as anarchy and self-help.

---

### 3.1 The WW1

---

Foreign HUMINT that targeted Britain during World War 1 (WW1) was a major issue for the UK. MI5 was tasked with countering German spies that maintained a presence in the UK. According to British Intelligence expert, Christopher Andrew ‘MI5 rounded up all the agents of any significance working for German naval intelligence’ (2018). Of the 120 spies sent to Britain to engage in espionage during the war, MI5 detected and apprehended 65 of them (Andrew, 2018). Besides espionage, Germany was attempting to

cajole and persuade foreign nations such as Mexico to join the war and align themselves with the Kaiser. Fortunately for Britain, counterintelligence methods at the time were not solely based on HUMINT. Contemporarily, some may associate the interception of messages with modern methods of GCHQ or another intelligence service. The ability to intercept messages has been around for some time, although to different degrees of efficiency and technique. According to the NSA, British intelligence managed to bottleneck the route that German communications travelled, in order to then step up cryptographic work on intercepting messages. As described by the NSA:

*On the first day of the war, the British cut Germany's transatlantic telegraph cable, compelling the Germans to send all telegrams to the Western Hemisphere via neutral countries or via cables that actually passed through territory controlled by their enemies. At the same time, the British government accelerated the development of a cryptographic office whose purpose it would be to read enemy traffic. This organization came to be known as Room 40 (NSA, n.d.[b], p.1).*

As it turned out, the government of Sweden was transmitting messages for Germany via South America, which attracted attention and targeting from British intelligence (NSA, n.d.[b], p.2). British intelligence tapped Swedish cables and managed to intercept the German Foreign Ministers (Arthur Zimmermann) encoded message to the president of Mexico (DocsTeach, n.d.). Plans to begin 'unrestricted submarine warfare were revealed' in conjunction with a proposed alliance between Mexico and Germany became British knowledge (DocsTeach, n.d.).

Zimmerman proposed an alliance between Mexico and Germany in order to go to war with the US in return for 'generous financial support and an understanding ... that Mexico is to reconquer the lost territory in Texas, New Mexico, and Arizona' (DocsTeach, n.d.). At the time of discovery, Britain was eager to gain support in the war from the US. The decoded message was sent to Washington in a strategic move to sway the USG's perception of Germany and WW1. Eventually, the Zimmermann scandal was revealed to the US public as a necessary ploy to rally public support for entering WW1 on the side of Britain and her allies. The Zimmerman case is a key hallmark in history that demonstrates

the far reaches of surveillance operations decades before the cyber age had evolved into today's sophistication.

---

## 3.2 The WW2

---

British surveillance during WW2 manifested in different forms which were not always morally permissible. Upon the declaration of war in 1939, '70,000 UK resident Germans and Austrians became classed as enemy aliens' (Kershaw, 2015). Concerned that Hitler was using spies to help subvert the UK, Britain took aggressive measures to significantly curtail the risk of foreign nationals living in the UK collaborating with Nazi Germany. Internment camps were set up in Britain to house 'aliens' from enemy nations such as Germany and Austria (The National Archives (UK), n.d.[a]). Due to the pressure of rooting out HUMINT infiltration by foreign nationals, during '[WW1] and [WW2] both sides set up internment camps to hold enemy aliens – civilians who were believed to be a potential threat and have sympathy with the enemy's war objectives' (The National Archives (UK), n.d.[a]). However, before aliens were placed in internment camps, their lives were subject to monitoring and intense scrutiny by internment tribunals set up by the Aliens Department of the Home Office (Kershaw, 2015). Additionally, Kershaw points out that:

*The object was to divide the aliens into three categories: Category A, to be interned; Category B, to be exempt from internment but subject to the restrictions decreed by the Special Order; and Category C, to be exempt from both internment and restrictions (Kershaw, 2015).*

Interestingly large numbers of aliens (66,000) were placed in category C, however within the first two years of WW2 8,000 enemy aliens were deported to British colonies and the dominions (The National Archives (UK), n.d.[a]; Kershaw, 2015). Not quite a 'Bentham's *Panopticon*', but Britain's internment camps enabled the British to keep track of foreign individuals for the sake of national security (Foucault, 1991, p.200). In the US, similar measures were taken to keep a watchful eye over Japanese nationals living in America. In the aftermath of the Pearl Harbour attack by Japan's Air force, US President Franklin Roosevelt established the executive order 9066, which enabled military personnel and the Secretary of War to set up internment camps for people with Japanese



ancestry living in the US (Library of Congress, 2015). During WW2 the USG moved 'approximately 117,000 people of Japanese ancestry... to internment camps such as Manzanar' (Library of Congress, 2015). Aside from wholesale observations of foreign nationals, Britain took more advanced measures of surveillance to reach its desired outcomes during the war. Hard-pressed to convince the US to intervene on behalf of Britain during WW2, intercepting American signals as a means of understanding US opinion was an essential practice by British intelligence services. In the view of Kathryn Brown, 'the British were reading State Department signals while simultaneously seeking to involve the Americans more heavily in the war effort against Germany' (1995, p.449). Definitive indications are scarce on this matter; however, Brown has stated that the 'British were intercepting State Department material in both the late 1930s and in the second half of 1941' which were delivered to Churchill (1995, p.450).

On the other hand, it is safe to say that most British and American SIGINT and code-breaking endeavours were aimed at Nazi Germany and imperial Japan throughout WW2. In particular, the targeting of the German Enigma cryptographic machine was of great importance for the allies during the war. The Enigma was a powerful cypher machine for its time, which was utilised by Germany's armed forces during WW2 (Wright, 2017, p.295). For many years Polish cryptologists at the behest of 'Marian Rejewski, had been happily breaking the German military cypher machine, the Enigma' (Welchman, 1986, p.71).

Upon invasion by Germany, the team of Polish cryptologists felt compelled to hand over their knowledge and replicas of the Enigma contraption to the French and the British (Welchman, 1986, p.71). Eventually, the work of figures such as Alan Turing managed to break Enigma, to produce intelligence which at the time was referred to (secretly) as Ultra or the Ultra Secret (Aldrich, 2011, p.1). The device was called the Bombe. Moreover, by 1942, the Allies had begun capitalising on Ultra intelligence and sent information to commanders in various theatres of war (Welchman, 1986, p.71).

Ultra-intelligence was shared with WW2 ally Russia to help tip the battle of Moscow in Russia's favour. Research conducted by Bradley Smith has revealed that '[a] very heavy flow of British Ultra was passed to the Soviets between October and December 1941 during the Battle of Moscow' (1988, p.60). On the other hand, knowledge of a successful

US nuclear program convinced Russia that atomic espionage inside America was necessary. Having placed multiple agents inside the US, Soviet agents eventually infiltrated the Manhattan Project at Los Alamos and numerous secret sites which were at the time a Top-Secret project designed to create a nuclear bomb (US Department of Energy, n.d.[a]). As a result of successful Soviet infiltration, the first successfully tested Soviet atomic bomb was a replica of America's previously tested atomic bomb (Andrew, 2010, p.366).

---

### 3.3 The Cold War and the Vagaries of Intelligence Collection

---

As recently set out above, Soviet intelligence officers were heavily embedded in the US under different covers. Highly sensitive information that was gleaned by Soviet spies was first encrypted then sent back to Moscow through telegraphic cables (US Department of Energy, n.d.[b]). US efforts to decrypt Soviet messages were severely set back as the Soviets used 'One-time pad' system which meant that 'at least in theory, decrypting them should have been impossible' (US Department of Energy, n.d.[b]). Determined to break Soviet encryption, the US Army's SIGINT service in 1943 worked relentlessly on overcoming this issue. Gene Grabeel was tasked with organising and analysing thousands of encrypted Soviet messages (NSA, n.d.[c]).

After years of making breaks in Soviet diplomatic and KGB cyphers, the US armed forces stumbled across Soviet codebooks in Germany (NSA, n.d.[d]). In 1946 US linguist Meredith Gardner reconstructed the KGB codebook. Gardner began to translate 'a few messages including one about the atomic bomb' (NSA, n.d.[d]). The code name given to this effort was VENONA, which managed to gather almost '3,000 intercepted Soviet intelligence and other classified telegrams sent during the period 1940 to 1948' (Andrew, 2010, p.366).

VENONA became 'the most closely guarded intelligence secret on both sides of the Atlantic during the early [C]old [W]ar' predominantly due to the great extent at which Soviet spies had penetrated US institutions (Andrew, 2010, p.366). Cognisant of the security lapses that enabled the Soviets to penetrate the Manhattan nuclear project,

secrecy was vital. That being said, Meredith Gardner managed to identify previously fragmented Soviet messages (NSA, n.d[c]; NSA, n.d[d]). Also, Gardner managed to discover that ‘someone inside the War Department General Staff was providing highly classified information to the Soviets’ (FAS, n.d.[a]). Knowledge of Soviet penetration created an atmosphere of caution and paranoia within the UISC as VENONA decrypts highlighted that the Soviet Union had hundreds of Americans gathering intelligence for them (Soviet Union) (Aldrich, 2011, p.73; Andrew, 2010, p.366).

This was an even more urgent case as the leadership of the American Communist Party (CPUSA), was shown to be ‘hand-in-glove with the KGB’ (Andrew, 2010, p.366). As a result of such fear and paranoia, intelligence scholar Richard Aldrich has suggested that it took three years until US intelligence deemed it safe to tell President Truman about the VENONA project (2011, p.73). US intelligence was cautious about telling President Truman about the VENONA program because his predecessor, President Roosevelt (administration) was infiltrated by Soviet spies (Andrew, 2010, p.366).

Despite such defensive measures, Soviet spies still managed to be informed about VENONA, through Kim Philby, a British double agent (US Department of Energy, n.d.[b]). Eventually, in 1980, the NSA shut down the program, long after the Soviets changed their measures of communication and espionage. However, the Soviets were not the only ones that conducted espionage in dangerous circumstances. Throughout the Cold War, Western nations made several attempts to penetrate Soviet countries to retrieve vital intelligence.

Notable examples include the joint effort between the NSA, CIA and British Intelligence to build a tunnel underneath Soviet cables in East Germany to tap them and retrieve information during the early 1950s. According to the CIA, ‘[i]n the 1950s, before reconnaissance satellites and other sophisticated collection systems were operational, wiretaps were one of the important technical means for collecting intelligence about Soviet military capabilities’ (2012).

Consequently, in 1954 CIA chief Allen Dulles permitted the secret mission of covert underground digging and tapping of Soviet cables (CIA, 2012). The CIA’s mission eventually produced ‘50,000 reels of tape, 443,000 fully transcribed conversations,

40,000 hours of telephone conversations 6,000,000 hours of teletype traffic, 1,750 intelligence reports' within one year of the operation (CIA, 2012). However, Russian intelligence gained knowledge of the CIA's underground surveillance campaign as a result of a double agent inside MI6 called George Blake (CIA, 2012).

The modus operandi of intelligence operations fluctuated throughout the 20<sup>th</sup> century, irrespective of technological leaps. In other words, US and British intelligence made use of ELINT SIGINT HUMINT interchangeably to contend with the circumstances at the time. As mentioned in Chapter 2, Electronic intelligence (ELINT) a form of SIGINT, concerns 'the collection... of information on foreign, non-communications, electromagnetic radiations emanating from other than atomic detonation sources' (Office of the Historian, 1955). In accordance with Kroger's summarisation, ELINT is focused on non-communication electromagnetic radiation that is emitted from 'missiles and missile guidance devices... developmental laboratories and field testing stations working on electronic devices, radar, navigational aids, anti-aircraft and aircraft gun direction, air-to-air or air-to-ground identification signals' (2011). Knowledge of Soviet weapons systems was of great importance to US policymakers and the Pentagon during the Cold War since it helped to dispel the perceived gap between America and the Soviet Union's missiles capacity.

During the Cold War the NSA, the National Reconnaissance Office (NRO) and the Naval Research Lab played a prominent role in alleviating this fear by developing ELINT endeavours against the Soviet Union. Grab and Poppy were successful satellite ELINT programs that targeted the 'Soviet radar signals' (McDonald and Moreno, 2005, p.8). Intelligence ascertained from Grab and Poppy 'provided cues to the location and capabilities of radar sites within the Soviet Union' (McDonald and Moreno, 2005, p.22). In particular, Poppy Satellites were designed to gather radar emissions from Soviet Navy ships to provide a clearer intelligence picture of Soviet capabilities and deployments (FAS, n.d.[b], p.1). Poppy satellites were launched between 1962 and 1971. In the view of the NRO Poppy made a significant contribution to America's national security during the Cold War (2005, p.1).

---

### 3.4 Photoreconnaissance and America's Perceived Military Gap With the Soviet Union

---

Towards the end (and after) WW2, the Soviet Union made aggressive political and military expansions into Eastern Europe. At the end of WW2, nations such as Bulgaria, Romania, Hungary, Poland and eastern Germany were occupied by Soviet forces (The National WW2 Museum, n.d.). Soviet military, air and naval installations behind the Iron Curtain were of great concern for the US and its NATO Allies. In particular, the US was fearful of Russia's conventional and non-conventional (atomic) capacity to strike key Western allies and the US mainland. Considering the fact that Russia had successfully test-fired its first atomic weapon in 1949, Washington was deeply troubled by Moscow's ballistic missile capability.

The two post-WW2 superpowers (the Soviet Union and America) engaged in an arms race to build the most formidable short and long-range missiles, nuclear weapons, discrete reconnaissance, attack aircraft, as well as radar systems and submarines. Throughout the 1950s foreign policy and intelligence analysts in the US were unsure as to whether or not the Soviet Union encompassed superior military capabilities that would leave America's national security in great peril (Bird and Bird, 2013, p.51-54). Intelligence gathering, therefore, became a quintessential tool to help the US to determine a clear picture of Soviet intentions regarding managing global affairs and its actual capacity to wage war. Photoreconnaissance was a form of Intelligence that the US regularly used throughout the world to take pictures of foreign national security assets.

Photoreconnaissance played a significant role in America's ability to determine if a gap in missile capabilities existed concerning the Soviet Union. In May 1960, during a Senate hearing, Director of the CIA Allen Dulles declared that as a result of U-2 spy plane photography:

*[W]e now have hard information about the nature, extent, and in many cases, the location of the Soviet ground – to –air missile development. We have learned much about the basic concept, magnitude, operational efficiency, deployment, and rate of development of the Soviet air defence system, including their early warning radar development...we have obtained new and valuable information with regard*

*to submarine deployment and the precise location of their submarine pens. In the opinion of our military, of our scientists, and of the senior officials responsible for our national security, the results of the program have been invaluable (CIA, 1975, p. 9-10).*

However, after a U-2 spy plane was shot down by the Soviet Union in 1960, President Eisenhower suspended surveillance flights over Russia. Faced with the disastrous outcome of a significantly reduced supply of vital information, the CIA devised new ways to conduct photographic surveillance over the Soviet Union. Much like Grab and Poppy, CORONA was a Top-Secret CIA and US Air Force (USAF) photographic satellite program that ran from August 1960 and May 1972 to gather intelligence on Soviet targets (National Geospatial-Intelligence Agency, n.d.[a]).

Once the Satellite was in orbit, pictures were taken then sent to Earth. In total, CORONA managed to capture over 800,000 images to plug the intelligence gap (CIA, 2015). CORONA thus played an integral role to help plug the gap in intelligence as a result of suspended reconnaissance flights over the Soviet Union. Moreover, In the case of the Soviet Union's international endeavours, America was keen to observe and gain concrete proof about the exact whereabouts of Soviet radar systems, Surface to Air Missiles (SAM), submarine location, and other sensitive national military assets. Photoreconnaissance was carried out by human-crewed covert spy planes such as the U-2 and its replacement A-12 OXCART or by satellite photoreconnaissance programs such as CORONA (National Geospatial-Intelligence Agency, n.d.[b]).

The Cuban Missile Crisis serves as an integral example of America's national security being predicated on the ability of U-2 spy planes to engage in dangerous but fruitful photoreconnaissance. In the early 1960s both the Soviet Union and Cuba's leader Fidel Castro were convinced that the US would invade Cuba in order to restore the Island to an acquiescent and subjugated partner in the Western Hemisphere. To alleviate and deter any potential US aggression, the Soviet Union transferred SAM and lethal nuclear warheads that could reach the US mainland. Pulling off such an audacious scheme required Russia to engage in a policy of deception. The element of denial came in the form of Russian government ministers assuring President Kennedy that Russia was only supporting a defensive military posture (John F Kennedy Presidential Library and

Museum, n.d.). Soviet deception was highlighted in President Kennedy's speech that outlined his infamous policy of quarantining Cuba to which President Kennedy stated that:

*The Soviet Government publicly stated on September 11, and I quote, "the armaments and military equipment sent to Cuba are designed exclusively for defensive purposes," ... Only last Thursday, as evidence of this rapid offensive buildup was already in my hand, Soviet Foreign Minister Gromyko told me in my office that... Soviet assistance to Cuba... "pursued solely the purpose of contributing to the defense capabilities of Cuba," that... "training by Soviet specialists of Cuban nationals in handling defensive armaments was by no means offensive (John F Kennedy Presidential Library and Museum, n.d.)*

The deception came in the form of denying the USG information concerning the surreptitious transfer of offensive weapons. Containing this secret plan proved to be difficult for the Soviet Union. US intelligence began to track Soviet movements in the region. In retaliation, the CIA (In 1962) requested to increase the flight coverage of Cuba. Towards the end of August in 1962, photographic evidence obtained from a U-2 spy plane flyover contributed to the discovery of at least 8 SAM in the Western portion of Cuba (Pedlow, and Welzenbach, 1992, p.208). Additional U-2 flyovers for the following month also provided concrete photographic evidence of more SAM sites and a then recently deployed Soviet aircraft (MiG-21) (Pedlow, and Welzenbach, 1992, p.208). Despite such crucial evidence being obtained, it is worth noting that the presence of SAM convinced the CIA and the USG that U-2 flights were incredibly dangerous because the Soviet Union shot down Francis Gary's U-2 spy plane in 1960 which subsequently led to his death (Pedlow, and Welzenbach, 1992, p.208).

Flights were reduced and only carried out when the circumstances, i.e. weather forecast would allow the US to obtain the best quality image possible (Pedlow, and Welzenbach, 1992, p.212). In a turn of events, during mid-October 1962 the weather over Cuba had cleared up, paving the way for a U-2 flyover. Photographs taken had revealed that the Soviet Union was building 'offensive nuclear missile bases' which lead to the deployment of 100,000 US troops to Florida and 180 vessels to the Caribbean in the event of a full-scale invasion of Cuba (National Archives and Records of Administration, 2017[a]).

Although journalists and other sources of HUMINT had spotted Russian soldiers in Cuba, without definitive evidence of a Soviet military build-up on the Island that came from photoreconnaissance, it may have been difficult for US policymakers to confidently form a timely pragmatic and targeted response. To an extent, Photoreconnaissance played a crucial role in highlighting the Soviet Union's scheme of undermining US dominance in the Western Hemisphere. In the view of the National Geospatial-Intelligence Agency, intelligence provided by U-2 photographic reconnaissance was a vital tool that helped to shape foreign policy by key decision-makers in the USG (National Geospatial-Intelligence Agency, n.d.[c]).

---

### **3.5 IGLOO WHITE and ELINT During the Vietnam War**

---

Reconnaissance took a technological turn in the Vietnam War to include sophisticated sensors to help the US track insurgents on the ground. During the Vietnam War, the famous Ho Chi Minh trail was used by communist forces as a supply line from North Vietnam through Laos and Cambodia into South Vietnam. Frustrated by communist resistance, the US introduced an electronic tracking system called 'IGLOO WHITE' to monitor enemy movements across the Ho Chi Minh trail (Rosenau and Long, 2009, p.29). IGLOO WHITE was an ELINT program that comprised of seismic and acoustic sensors that were deployed along the Ho Chi Ming Trail (Rosenau and Long, 2009, p.29; National Museum of the US Air Force, 2015). Data retrieved was sent back to 'Nakhon Phanom Royal Thai Air Force Base' where it was analysed to detect enemy movements (Rosenau and Long, 2009, p.15).



---

## 3.6 OPERATION SOLO and The FBI's HUMINT Mole

---

So far, multiple examples of surveillance gathering have demonstrated a considerable amount of skill and finesse. However, the FBI's OPERATION SOLO remains a stand out high-risk HUMINT program that had a significant impact on America's ability to infiltrate some of the highest ranks in the Chinese and Soviet Union's Communist Party. Operation SOLO was an FBI HUMINT mission that persuaded two brothers, Morris and Jack Childs, to penetrate the Soviet Union and China to engage in personal conversations with Khrushchev and Mao Zedong (National Security Archive (US), 2012). For the sake of clarity, both brothers together were codenamed SOLO (National Security Archive (US), 2012). Throughout the FBI's vault, the codename CG 5824-S is used to describe a SOLO informant. The FBI achieved this great accomplishment by convincing the dissatisfied communist's Morris Child and Jack Child who previously left the CPUSA, into becoming FBI informants that rejoined the party (National Security Archive (US), 2012).

Declassified documents concerning Operation SOLO have revealed some startling facts about the nature of the program. As stated earlier, CG5824-S managed to penetrate some of the highest ranks in both China and the Soviet Union. The value of such excellent intelligence work was that the informant was able to meet Soviet and Chinese officials and learn about the overall posture towards the US and what they thought of America at the time. In one document it was noted that President Mao opened up to CG5824-S, in a two-hour discussion:

*[H]e told the informant that the main enemy of communism is the US. He stated that the workers need a strong communist party in the US. He said that government oppression against the [CPUSA] will make it a stronger party. He stated that US seems afraid of a big war, yet it will not even fight little wars... He said the US imperialism is not sure of itself, it faces many difficulties... He said China is not worried about getting into the UN and that the other countries will come begging to China to join the UN (FBI, 1958[a], p.63).*

Moreover, Operation Solo revealed to the USIC the lengths the Soviets were willing to go, to see communism thrive across the US. Accordingly, from 1958 to 1968, the Soviet Union provided a total of \$5,736,538.09 to the CPUSA (FBI, 1968[a], p.17). Furthermore, in 1958, the FBI came to the agreement that they should ‘attempt to fully capitalize upon this situation and...guide one of our informants into the position of being selected by the CPUSA as a courier between the party in this country and the Soviet Union’ (1958[b], p.1). This proved to be a successful decision as months later a summary of CG 5824-S notes revealed that he (CG 5824-S) ‘furnished the following address which he is to use for the purpose of sending documents of the Communist Party - USA to Communist Party of China: TANG MING-CHAO, 9 Tai Chi Chang, Pecking, China’ (FBI, 1958[a], p.68).

The informant also ‘furnished the following address which he is to use for the purpose of sending documents from the Communist Party – USA to the Communist Party of the Soviet Union: Main Post Office Box 341, Moscow, Russia’ (FBI, 1958[a], p.68). This revelation immediately alerted the FBI to the Soviet and Chinese determination to assist and guide the CPUSA. Operation SOLO demonstrates that less sophisticated forms of intelligence can be just as effective as advanced contraptions that can intercept government messages.

---

### **3.7 COINTELPRO, Black Extremism and the FBI’s Domestic Psychological Warfare**

---

During the American civil rights period, the USG became concerned with the litany of organisations that were beginning to influence the black community. As a consequence, the FBI was tasked with conducting domestic surveillance and a psychological warfare counterintelligence program against various groups. This counterintelligence program became known as COINTELPRO. Targets included the Black Panther Party, the Student Nonviolent Coordination Committee, the Southern Christian leadership conference, Revolutionary Action Movement (RAM), the deacons for defence and justice, Congress of Racial Equality, the Nation of Islam and various other student and local organisations. COINTELPRO aimed to ‘[p]revent the rise of a “messiah” who could unify and electrify, the militant Black Nationalist movement. Malcolm X might have been such a “messiah;” he is the martyr of the movement today’ (FBI, 1967, p.69). Other contenders included

‘Martin Luther King Stokely Carmichael and Elijah Muhammad...King could be a very real contender for this position should he abandon his supposed "obedience" to white liberal doctrines (nonviolence) and embrace Black Nationalism’ (FBI, 1967, p.69).

However, the case of Martin Luther King (MLK) reads like something from a JTRIG playbook, albeit with less technologically savvy methods. During the civil rights period, J Edgar Hoover began to fear MLK. Hoover made it clear that the FBI ‘must mark him now [MLK], if we have not done so before, as the most dangerous Negro of the future in this Nation from the standpoint of [C]ommunist, the Negro, and national security’ (National Archives and Records Administration (US), 2016). As a result, the FBI launched a crusade to gather information on MLK through electronic surveillance and informants. According to the National Archives and Records Administration (US) during the early 1960s, the FBI placed MLK under electronic surveillance, which was authorised by the former Attorney General Robert Kennedy (2016). Eventually, surveillance paid off when it came to the attention of the FBI that MLK was allegedly engaging in an extramarital affair(s). To ratchet up the pressure on MLK, the FBI sent an anonymous letter detailing the awareness of his affair in conjunction with ‘a copy of an electronic surveillance tape’ (National Archives (US), 2016).

KING.

In view of your low grade, abnormal personal behavior I will not dignify your name with either a Mr. or a Reverend or a Dr. And, your last name calls to mind only the type of King such as King Henry the VIII and his countless acts of adultery and immoral conduct lower than that of a beast.

King, look into your heart. You know you are a complete fraud and a great liability to all of us Negroes. White people in this country have enough frauds of their own but I am sure they don't have one at this time that is any where near your equal. You are no clergyman and you know it. I repeat you are a colossal fraud and an evil, vicious one at that. You could not believe in God and act as you do. Clearly you don't believe in any personal moral principles.

King, like all frauds your end is approaching. You could have been our greatest leader. You, even at an early age have turned out to be not a leader but a dissolute, abnormal moral imbecile. We will now have to depend on our older leaders like Wilkins a man of character and thank God we have others like him. But you are done. Your "honorary" degrees, your Nobel Prize (what a grim farce) and other awards will not save you. King, I repeat you are done.

No person can overcome facts, not even a fraud like yourself. Lend your sexually psychotic ear to the enclosure. You will find yourself and in all your dirt, filth, evil and moronic talk exposed on the record for all time. I repeat - no person can argue successfully against facts. You are finished. You will find on the record for all time your filthy, dirty, evil companions, male and female giving expression with you to your hideous abnormalities. And some of them to pretend to be ministers of the Gospel. Satan could not do more. What incredible evilness. It is all there on the record, your sexual orgies. Listen to yourself you filthy, abnormal animal. You are on the record. You have been on the record - all your adulterous acts, your sexual orgies extending far into the past. This one is but a tiny sample. You will understand this. Yes, from your ferocious evil playmates on the east coast to \_\_\_\_\_ and others on the west coast and outside the country you are on the record. King you are done.

The American public, the church organizations that have been helping - Protestant, Catholic and Jews will know you for what you are - an evil, abnormal beast. So will others who have backed you. You are done.

King, there is only one thing left for you to do. You know what it is. You have just 34 days in which to do (this exact number has been selected for a specific reason, it has definite practical significance. You are done. There is but one way out for you. You better take it before your filthy, abnormal fraudulent self is bared to the nation.

Figure 10: Electronic Frontier Foundation, 2014

Excerpts from the letter (see figure 10) aggressively stated that:

*Satan could not do more. What incredible evilness. It is all there on the record, your sexual orgies. Listen to yourself you filthy, abnormal animal. You are on the record... all your adulterous acts, your sexual orgies extending far into the past... The American public, the church organisations that have been helping – Protestant, Catholic and Jews will know you for what you are – an evil, abnormal beast...you are done. King there is only one thing left for you to do. You know what it is...There is but one way out for you (EFF, 2014[b]).*

Judging from the extract cited above, it is clear that this letter aimed to create a vortex of doubt within MLK and trigger the desire to remove himself from the civil rights movement. This is a particularly important point considering how highly feared MLK was by the FBI in terms of his ability to influence the African American population and white liberals. Additional groups such as the Revolutionary Action Movement (RAM) in Philadelphia were targets of surveillance and psychological warfare tactics by the FBI's COINTELPRO. Although specific names are heavily redacted within the documents on RAM, members that had begun proselytising RAM ideology in Philadelphia were placed under surveillance by the police (FBI, 1967, p.7).

Tracking RAM members was an essential part of the FBI's attack on this organisation as they aimed to frustrate and deter RAM activity. Surveillance and psychological tactics consisted of local police searching for RAM members and stopping their cars to make it clear to RAM that their presence was going to be challenged (FBI, 1967, p.7). To exacerbate the feeling of frustration, the FBI would target RAM members by continually arresting them. For example, in an excerpt from a declassified file, the FBI stated that a RAM member:

*[W]as located passing out RAM literature at a local school. He was interrogated. He was arrested as a narcotic user on the basis of alleged needle marks. He was fingerprinted and photographed. He was subsequently released by a magistrate. Any excuse for arrest was promptly implemented by arrest. Any possibility of neutralizing a RAM activist was exercised (FBI, 1967, p.7).*

Other tactics of the FBI manifested in the cycle of arrest and release of RAM members until they ran out of money to pay for bail. Accordingly, ‘RAM people were arrested and released on bail, but were re-arrested several times until they could no longer make bail’ (FBI, 1967, p.8). Much to the joy of the FBI, in 1967 it was noted that ‘local actions appear... to have curtailed the activities of this group. It was apparently a highly frustrating experience for the persons involved’ (1967, p.8). This document went on to state that a RAM member who had previously been harassed was informed ‘that he was again under arrest and that his wife and sister were also under arrest’, which resulted in the RAM member to ‘beat the floor with his fists’ and cry (FBI, 1967, p.8).

Albeit a crude tactic, this was an ingenious plan to subdue RAM members. According to the FBI, as a result of RAM members not being able to make bail RAM leaders spent large portions of the summer incarcerated leading to a decrease in violence conducted by RAM (1967, p.68). With crucial leaders in jail, the message was made clear to local RAM members; join RAM, and he or she will risk being targeted and harassed until jail and the police become a regular sight. In this sense, psychological warfare can be waged in conjunction with surveillance methods to meet the desired goal against targets.

---

### 3.8 The 21<sup>ST</sup> Century

---

So far, surveillance methods have included HUMINT, SIGINT ELINT and the tapping of cables. In contrast, 21<sup>st</sup>-century cyberspace is structured in such a way that those who use the Internet often leave a matrix of digital footprints for lay individuals or intelligence services to follow. Digital footprints can manifest in the form of communications data or metadata. The UK government defines communications data as, ‘the context, but not the content of a communication: who was communicating, when, from where, and with whom’ (House of Commons, 2015[c], p.1). Succinctly put ‘Communications data is the ‘who’, ‘when’, ‘where’ and ‘how’ of a communication’ (House of Commons, 2015[c], p.1).

For example, an unwitting civilian could set up a drug deal on his or her phone not realising that the message sent can be tracked and analysed in terms of the date a message was sent, the location in which the individual sent the message and to whom it was sent. As expressed by Keith Bristow the Director-General of the National Crime Agency,

‘Communications data is still overwhelmingly the most powerful tool available to those investigating child sexual exploitation and identifying and safeguarding its victims and potential victims’ (Bristow 2015, House of Commons, 2015[c], p.1). Therefore in the 21<sup>st</sup>-century communications data is an integral part of solving crimes and boosting national security.

Furthermore, modern forms of surveillance require telecommunications companies to comply with or submit to government requests for information (communications data) that are of great value to intelligence services. In light of the evidence provided by Rainey Reitman, in 2016 alone ‘the United States government sent at least 49,868 requests to Facebook for user data. In the same period, it sent 27,850 requests to Google and 9,076 to Apple’ (Facebook, 2016, cited in Reitman, 2017).

However, the Snowden revelations revealed a more aggressive approach taken by the USG. In Greenwald’s book *No Place to Hide*, NSA programs such as PRISM allow the agency to ‘collect data directly from the servers of nine of the biggest [I]nternet companies’ (2014[b], p.108). In reference to a slide from the NSA, the PRISM program alludes to the alleged ‘collection directly from the servers of these U.S. service providers: Microsoft, Yahoo, Google Facebook, PalTalk, AOL, Skype, YouTube Apple’ (Greenwald, 2014[b], p.108).

Moreover, modern British laws have also put a considerable amount of pressure on private telecommunications companies to help the state conduct relevant surveillance on targets. On the 8<sup>th</sup> April 2014, the ECJ ruled against its previous Directive ‘2006/24/EC’ where article 6 stated that communications companies could retain data ‘for periods of not less than six months and not more than two years from the date of the communication’ (EUR-LEX, 2006). The ECJ concluded that the data which is retained makes it possible to:

*[T]o know the identity of the person... to identify the time of the communication as well as the place from which that communication took place and...to know the frequency of the communications...Those data, taken as a whole, may provide very precise information on the private lives of the persons whose data are retained, such as the habits of everyday life, daily or other movements... social*

*relationships and the social environments* (Court of Justice of the European Union, 2014, p.1).

Therefore, the ECJ ruled that the previous 2006 directive violates fundamental rights concerning the respect for privacy which may conjure a gripping sense of constant surveillance (Court of Justice of the European Union, 2014, p.1-2). With the UK government concerned about national security and the potential loss of valuable communications data; the Conservative Party rushed DRIPA through Parliament to essentially override the EU's ruling and force companies operating in Britain to maintain their previous practice of holding on to data for up to two years.

As a result, to date, the IPA (following on from DRIPA) states in section 87 that, '[a] retention notice must not require any data to be retained for more than 12 months' (*Investigatory Powers Act, 2016*, p.83). In the 21<sup>st</sup> century, such mandates or laws are deemed as necessary by governments and law enforcement to protect the nation against criminals. Furthermore, in the case of encryption removal and Britain's recent 2016 IPA, the Conservative government has mandated that it can deliver a 'technical capability notice that would impose any obligations relating to the removal by a relevant operator of electronic protection applied by or on behalf of that operator to any communications or data', as defined in section 255 (*Investigatory Powers Act, 2016*, p.221).

Aside from compelling Internet service providers to store data, surveillance can be conducted in far more sophisticated ways. In recent history, The Intercept has reported on GCHQ's more aggressive approach in overcoming encryption in the form of covert interception of encryption keys from telecommunications companies. As cited by The Intercept, 'American and British spies hacked into the internal computer network of the largest manufacturer of SIM cards (Gemalto) in the world, stealing encryption keys used to protect the privacy of cellphone communications across the globe' (2015[d]). Gemalto is a multinational company which manufactures 2 billion SIM cards a year for clients such as 'AT&T, T-Mobile, Verizon, Sprint and some 450 wireless network providers around the world' (The Intercept, 2015[d]). By stealing encryption keys, theoretically, GCHQ would be able to break into a sizable amount of phones. One GCHQ document that was cited by The Intercept asserted that key harvesting methodology is predicated on collecting 'Ki values in transit between mobile network operators and SIM card



personalisation centres. Provisioning information is often sent between these organisations by email’ to which British spies began to target (2015[e], p.4).

Figure 11 highlights the list of emails that GCHQ was interested in, in conjunction with their mission of harvesting encryption keys. One individual in particular located in Thailand was a sales a manager for Gemalto that was seen by GCHQ ‘sending PGP – encrypted output files in XKEYSCORE’ (The Intercept, 2015[f], p.1). Accordingly, GCHQ concluded that this might ‘be a good place to start’ in terms of surveillance (The Intercept, 2015[f], p.1).

- Findings from ██████████

JTRIG research identified ██████████ as a Gemalto Technical Consultant in Prague. Searching in UDAQ revealed an item in which an email was sent from sharing@yuuwaa.com to a number of @gemalto.com email addresses, including ██████████ and ██████████ (who is already known to us as a Tech Consultant). Investigation on the internet revealed that Yuuwaa (www.yuwaa.com) is a device for storing and sharing files sold by Gemalto. It consists of a USB stick and associated management software. The device also provides access to online storage using a subscription model. It claims to use 128-bit SSL to encrypt the traffic to the online storage location. The device is aimed at the general consumer market, so presumably Gemalto is encouraging its employees to use it. Amusingly, the quotes from “customers” on the website all appear to be from Gemalto employees!

██████████ is a Gemalto employee in Singapore. His job title is “Sales – Telecom Solutions and Services”. He will shortly (Feb/March 2011) be moving to Paris (still with Gemalto)

██████████ is described as a “Consumer Device – Product Marketing Manager” at La Ciotat (France). He appears to be some sort of administrator for Yuuwaa, and we have not seen any indication that he will have any data of interest, so he is unlikely to be worth following up.

██████████ is “Technical Account Manager METNA-Telecom” and is based in Dubai (from previous knowledge). We did not see any interesting data in collection, and since we have good coverage of the Dubai office, further investigation is probably unnecessary at this time.

██████████ is “CITO T&I Servers Software/Cloud Computing Innovation WG Chairman” and is not likely to be of interest.

██████████ is Account Manager (Middle East) and is based in Dubai (see ██████████)

██████████ appears to be Sales Manager for Gemalto (Thailand). We saw him sending PGP-encrypted output files in XKEYSCORE. Again, if we ever become more interested in this area, he would certainly be a good place to start.

All other names (other than ██████████ who was already known about) did not have any useful information or any details of their role.

For a full list of names, see the CMAPS (██████████ contacts) under OP HIGHLAND FLING.

- Hopefully some of this information will be useful in future efforts against Gemalto.

Figure 11: The Intercept, 2015[f], p.1

Moreover, GCHQ test trialled some of the goals mentioned above, and the organisation managed to obtain encryption keys of network providers in India, Afghanistan, Yemen and Iran (The Intercept, 2015[d]). At this juncture, it is clear to see a distinction or increase in sophistication between 20th-century examples and GCHQ’s current activities. This example marks a significant difference in previous methods of tapping cables.

An additional and more Orwellian example of surveillance revolves around documents provided to The Intercept by Snowden. The NSA encompasses a global surveillance

apparatus that engages subjects via implants, also known as malware (The Courage Foundation, 2014[b]). Malware is defined as ‘a type of computer program designed to infect a legitimate user's computer and inflict harm on it in multiple ways’ (Kaspersky, 2019[c]). Put rather sarcastically by news outlet the Medium; the ‘NSA has malware of all flavors’ (2016). To name a few VALIDATOR, UNITEDRAKE, STRAITBIZARRE, SCHOOLMONTANA, SIERRAMONTANA, are all variants of malware that can subvert network security (Medium, 2016). Additionally, one of the most chilling concerns highlighted in the Snowden leaks was the NSA’s Artificial Intelligence (AI) hacking initiative (see figure 12).

As held by the NSA, TURBINE is an automated program that ‘manages the active implants that make up the Active SIGINT system’ to infect more targets (The Courage Foundation, 2014[b]). Attacking targets at scale is an issue for the NSA because human operatives unintentionally reduce the scope for large operations due to the perception that humans at times fail to see the bigger picture (The Courage Foundation, 2014[b]). With regards to the capacity of TURBINE, implant networks can scale up to the millions due to the automated aspect of TURBINE (The Courage Foundation, 2014[b]).

(TS//SI//REL) TURBINE manages the active implants that make up the Active SIGINT system. Active SIGINT offers a more **aggressive** approach to SIGINT. We retrieve data through intervention in our targets’ computers or network devices. Extract data from machine. This is: Tailored Access Operations!

One of the greatest challenges for Active SIGINT/attack is **scale**. Human “drivers” limit ability for large-scale exploitation (humans tend to operate within their own environment, not taking into account the bigger picture)

The TURBINE infrastructure will allow the current implant network to scale to large size (millions of implants) by creating a system that does **automated control implants by groups** instead of individually.

**Expert System** (resource and operations manager) is like the **brain** it manages the applications and functions of implants.  
 Decides which tools should be provided to a given implant and executes the rules on how it should be used  
 Decisions of the expert system are passed to the **command and control modules**, which execute the decision against the appropriate set of implants.

**Diode** is a device that allows connectivity from the high side to the low side network without human intervention.

Figure 12: The Courage Foundation, 2014[b]

In reference to the scale of the NSA’s infection infrastructure, cybersecurity expert Mikko Hypponen has stated that ‘[i]t couldn’t possibly be targeted and named. It sounds like wholesale infection and wholesale surveillance’ (Greenwald and Gallagher, 2014). This truly is a wholesale surveillance and infection program considering that back in 2004 ‘small network of only 100 to 150 implants’ (Hypponen, 2014, cited in Greenwald and Gallagher, 2014). What is more concerning is that the NSA’s capabilities would have increased significantly since 2004. Although I can only speculate at this moment in time,

it is highly likely that if such an AI program still exists, it will be far more superior to Turbine's capabilities.

To conclude, it is important to note that despite the sizable changes in how intelligence is done, sometimes simple methods of espionage are still just as successful. For example, Ana Belen Montes, a prolific Cuban analyst for the Defense Intelligence Agency (DIA) was arrested days after 9/11 for spying on behalf of the Cuban Government (FBI, n.d.[b]). Montes did not download any files like Snowden nor did she pilot a U-2 spy plane. Instead, Montes simply memorised sensitive information that she had clearance to read. According to the FBI, Montes 'kept the details in her head and went home and typed them up on her laptop. Then, she transferred the information onto encrypted disks' (n.d.[b]).

This is a crucial example of why it is necessary to not fall into the trap of assuming that simple methods of espionage are not just as successful as more complex forms. Moreover, it is also worth noting that the NSA's upstream program is not so different from Britain's previous surveillance activity that discovered the Zimmerman telegram. Under programs such as Upstream, 'the NSA tapped into privately owned fibre-optic cables carrying information to and from the United States to conduct surveillance on foreign targets' (Fidler, 2015, p.97). Although the specifics of how a cable is tapped would have changed somewhat over time, the concept of tapping cables is still a prominent means of acquiring vast amounts of information. Overall, the evolution of surveillance methods and events have changed dramatically, particularly in the cyber age. Nonetheless, this does not extirpate old practices.

---

## 3.9 The Evolution of Propaganda from the 20<sup>th</sup> to the 21<sup>st</sup> Century

---

Throughout the 20<sup>th</sup> century, propaganda was not strictly conducted in one particular way via one specific delivery route. Nations used a whole range of means to influence foreign and domestic audiences as opposed to relying on a specific method of delivery for a particular period. Nonetheless, this chapter aims to explore how propaganda has been used and developed throughout the 20<sup>th</sup> and 21<sup>st</sup> century. While it is essential to highlight that propaganda and the influencing of public opinion is an age-old international practice, this chapter will only focus on British and American efforts. Despite what may initially appear to be a truncated scope, British and American propaganda efforts reached all corners of this planet. This chapter will focus on regions that were affected by British and American propaganda such as, Latin America, Europe and Africa in conjunction with domestic US propaganda carried out by the USG. When attempting to provide an etymology of propaganda, most academics point to the Vatican. Accordingly, '[i]n 1622 the Vatican described its missionary activities overseas as *Sacra Congregatio de Propaganda Fide*' (Koppang, 2009, p.117). Similarly, Raymond Dodge advocates the view that '[i]t was Pope Gregory XV who almost exactly three centuries ago after many years of preparation, finally founded the great Propaganda College to care for the interests of the Church in non-Catholic countries' (1920, p.242).

Before the 20<sup>th</sup> century, theatre and plays were prominent forms of propaganda, in conjunction with paintings. Moreover, at the advent of America's military intervention in Cuba's war of independence with Spain in 1898, Yellow Journalism contributed to reinforcing the notion that the US had a duty to intervene and protect Cuba from Spanish colonialism (Office of the Historian, n.d.[c]). Yellow Journalism was 'a style of newspaper reporting that emphasized sensationalism over facts' (Office of the Historian, n.d.[c]). Yellow Journalism was an effective type of communication which helped to foster support for the war in Cuba, the Western Hemisphere and other places in the world (Office of the Historian, n.d.[c]).

Conversely, WW1 marked a significant turning point in how propaganda was perceived and produced. As described in James Brown's book *Techniques of Persuasion*, 'there can be little doubt that the First World War represents the earliest occasion when...Propaganda became a fully-fledged instrument making use of a scientific approach which attempted some sort of objective technique' (1963, p.82). Indiscriminate targeting of civilians destroyed millions of lives, as opposed to previous wars that usually revolved around two or more armies fighting till death on a rugged patch of earth (The British Library, n.d.). As reflected in the work of Bernard Wilkin '[a]lthough the number of civilians killed by aerial machines remained small during the war, these air raids nonetheless caused widespread terror' on civilians during WW1 (2014).

Consequently, this meant that the morale of the citizens during the war was more important than ever, to which '[f]or the first time the barometer of public morale needed as much careful attention as the efficiency of the troops... this revolutionized attitudes to propaganda' (Haste, 1977, p.1). Put in another way; modern total wars saw anguish spread across the population; therefore propaganda was used to placate fear and stiffen the nations resolve to support the war. Overall, methods of propaganda varied throughout the war. Moreover, as literacy increased during the advent of the 20<sup>th</sup> century, propagandists sought to exploit this growing capacity. The view proposed by Edward Bernays advocates the above point concerning the literacy increase of citizens but from a scientific approach:

*Universal literacy was supposed to educate the common man to control his environment. Once he could read and write he would have a mind fit to rule. So ran the democratic doctrine. But instead of a mind, universal literacy has given him rubber stamps, rubber stamps inked with advertising slogans, with editorials, with published scientific data, with the trivialities of the tabloids and the platitudes of history, but quite innocent of original thought. Each man's rubber stamps are the duplicates of millions of others, so that when those millions are exposed to the same stimuli, all received identical imprints (Bernays, 2005, p.48).*



Figure 13: BBC, 2014

Posters served as stimuli that helped to shape public opinion during the turn of the century. In terms of recruitment, the infamous Lord Kitchener poster helped the UK build a formidable volunteer army of up to 3 million soldiers to fight during WW1 (Baines, and O'Shaughnessy, 2014, p.4). To a great extent, the Kitchener poster evoked a sense of patriotism at an instant because it symbolised duty to the state in very few words.

The ability to read these few words was key to helping the British government establish its psychological rubber stamps. Moreover, text-based leaflets dropped from aeroplanes played a significant role in influencing the morale of both troops and civilians. Lynette Finch has suggested that 'allied forces dropped... a total of twenty-six million propaganda leaflets aimed either at enemy troops or civilian populations' (2000, p.370). Targets were encouraged to turn against the war effort (Finch, 2000, p.371). Leaflets were vital in getting propaganda messages over enemy lines and establishing a form of communication with the civilians who may be already against the war.

Furthermore, censorship and the position played by Newspapers was pivotal for Britain's attempts to control information that had an impact on the morale of its citizens during

WW1 (Haste, 1977, p.2). Academics such as Davison suggested that Bribery of Newspapers was a common phenomenon in WW1 (1971. p.3). Additionally, Davidson has indicated that global powers spent a considerable amount of money to shape messages conveyed by the press to the public (1971. p.3). Considering that war rumours could influence people that are already in a desperate state, it is understandable to see why the UK government deemed it necessary to control what was displayed by the media. In retrospect, WW1 propaganda has become synonymous with the dissemination of gross lies or as it is commonly referred to today, atrocity propaganda. Atrocity propaganda was designed to ‘stiffen the fighting spirit of entire nations, to create fear of defeat, and, as a more practical means, to raise funds and encourage enlistment to halt these inhumane acts’ (Jowett and O’Donnell, 2011, p.225).

During WW1, atrocity stories contained in the notorious Bryce Report aggrandised the imagination of the British public concerning German atrocities (see chapter 8). According to Finch’s assessment of Bertrand Russell’s reaction to false propaganda stories concerning German warfare abuses, British propaganda ‘[signalled] the return to barbarism on the part of the eager readership and the newspapers who delighted in supplying the detail’ (2000, p.379). In allied nations, grotesque stories surfaced that the Germans were ‘crucifying prisoners of war, and using priests as clappers in cathedral bells’ (Brown, 1963, p.85). Atrocity propaganda was not a one-sided affair. Germany also took part in this foul game of false stories. Accordingly, ‘on the German side there were accounts of... the use of guerrillas and ‘savages’ from Africa and Asia to fight civilized peoples... on the part of the Allied troops’ (Brown, 1963, p.85). Similarly, Beaglehole has highlighted the temptations that governments faced to contort the truth:

*But the new methods of influencing the popular mind through the use of the press, the lecture platform, the advertising column, the wireless and the motion picture proved so immediately and astonishingly effective that, as the difficulties and dangers, the trials and temptations, of the war increased and military necessities became more compelling, these same methods soon came to be used with less and less scruple for truth and justice in order to keep the popular passions aroused to that fever heat of fear, anger and rage, without which the authorities believed it to be impossible to continue the relentless prosecution of a war that was exacting*

*such universal calamitous destruction, and inflicting such unspeakable agonies of suffering. It was under these circumstances that the word propaganda with all the sinister associations which it now arouses in the popular mind, came into common use (Beaglehole, 1928, p.93).*

Propaganda dissemination during WW1 is not as efficient as the mediums available in the 21<sup>st</sup> century; however, information campaigns wielded by both sides had a significant impact on public opinion.

---

### **3.10 OSS Propaganda during WW2: Eugenics and Overt Propaganda in Nazi Germany, America and Britain.**

---

Up until 1941, America remained neutral during WW2, although Washington often provided the British with military supplies to fight the war. Upon entry into the war, the US lacked a single intelligence service that ‘engaged in all basic secret activities: espionage, covert action, propaganda, and counterintelligence’ (CIA, 2013[b]). During the summer of 1942, ‘President Franklin Roosevelt created the Office of Strategic Services (OSS)... to collect and analyze strategic information and to conduct espionage and special operations’ (CIA, 2013[b]). The OSS took part in some of the simplest yet, paradoxically detailed forms of propaganda against foreign targets. However, black propaganda or psychological warfare was produced by the Morale Operations Branch, a subunit of the OSS (CIA, 2013[b]). Within the CIA’s declassified Morale Operations Field Manual, a plethora of information concerning the development of propaganda is evident. To begin with, the objectives of Morale Operations in an enemies country was to:

*To incite and spread dissension, confusion, and disorder; to promote subversive activities against his government by encouraging underground groups, and to depress the morale of his people...to encourage and assist in the promotion of resistance and revolt against Axis control by the people of these territories, and to raise their morale and will to resist (CIA, 2016[b], p.6).*



WW2 was a total war that affected civilians significantly throughout the world. As previously suggested, the distribution of propaganda was increased in order to shape the perception of WW2. Additionally, the OSS objectives were achieved through the:

*Manipulation of individuals and underground groups...Bribery and Blackmail...Rumors... forgery, to include the writing of poison-pen letters, forging of misleading intelligence documents, falsification of enemy documents and periodicals, and the printing of false orders to the enemy, regulations, and proclamations... false leaflets, pamphlets, and graphics, to be used for subversive deception within enemy and enemy-occupied countries...“Freedom stations” masquerading as the voice of groups resistant within enemy and enemy occupied countries (CIA, 2016[b], p.7).*

Unlike the military that dropped hundreds of thousands of leaflets, ‘mass means of communication’ was not authorized by the Morale Operations Branch (CIA, 2016[b], p.7-8). Instead, the aim was to place relevant propaganda to important figures who could influence large audiences (CIA, 2016[b], p.8). Popular figures included ‘key enemy military and naval personnel, administrators, civil leaders, quislings, diplomats, and potential leaders of resistance’ (CIA, 2016[b], p.8). In the case of forgeries, the forged documents needed to end up in the hands of enemy soldiers and the police (CIA, 2016[b], p.31).

The rationale behind this objective was to create or inflame already existing fracture points among the military and police. However, for this to take place, intelligence briefings on individuals and groups was necessary to provide a crucial picture of key influencers and their personal beliefs. Forgeries of high-value German targets were produced by ‘an ex-con artist who was known only as “Jim.”...could fake the signatures of Adolf Hitler, Heinrich Himmler, Benito Mussolini, and other US enemies’ with incredible accuracy (CIA, 2013[c]).

Moreover, specific examples of OSS propaganda provided by contemporary CIA accounts include Operation HEMLOCK, an endeavour in which US intelligence sent anonymous and malicious poison-pen letters to the Gestapo and the families of dead German servicemen (CIA, 2013[b]). Poison-pen letters that were sent to deceased family

members sought to imply that German servicemen had been killed by a lack of coherent medical treatment as a means of inflicting terror within the civilian populace (CIA, 2013[b]). While deadly air raids were necessary to destroy targets and reduce the will to fight, propaganda in the form of poison pen letters was an auxiliary form of propaganda to break the will of civilians to support the war.

Undoubtedly, this thesis aims to cover the vast scope of covert propaganda that has been wielded by British and American intelligence services. In doing so, there is a great risk of excluding the influence of overt imagery that was used by democratic nations such as the US, Britain and genocidal anti-democratic countries, i.e. Nazi Germany. Although Nazi Germany was ideologically opposed to the liberal democratic values shared by Western states, the antecedent of Nazi Germany's desire to shape the genetics of its citizens had its roots in the UK and was widely celebrated in the US and Scandinavia (Roll-Hansen, 1989, p.335-337). A comparison between Nazi Germany and Western democratic nations may cause confusion considering the scale at which the Nazi's murdered over 6 million Jews. Furthermore, it is vital to point out that eugenics was discussed in Germany before the rise of the Third Reich (Dietrich, 1992, p.577).

Aside from the obvious difference between the Nazi's and the US, beginning in 1909 to 1963 within the state of California "20,000 sterilizations took place in state institutions, comprising one-third of the total number performed in the 32 states where such action was legal" (Estrada, 2015). Before the rise of Hitler, the US had embraced the ideas of social and racial purification by enforcing eugenics laws and propaganda campaigns to rationalise heinous acts of forced sterilisations. Similarly, in 1907 Sibyl Gotto and Francis Galton created the Eugenics Society in the UK. The (UK) Eugenics Society attempted to influence legislation on forced sterilisation in Parliament but ultimately failed to leverage enough influence (propaganda) to pass the bill (Wellcome Library, 2019[a]).

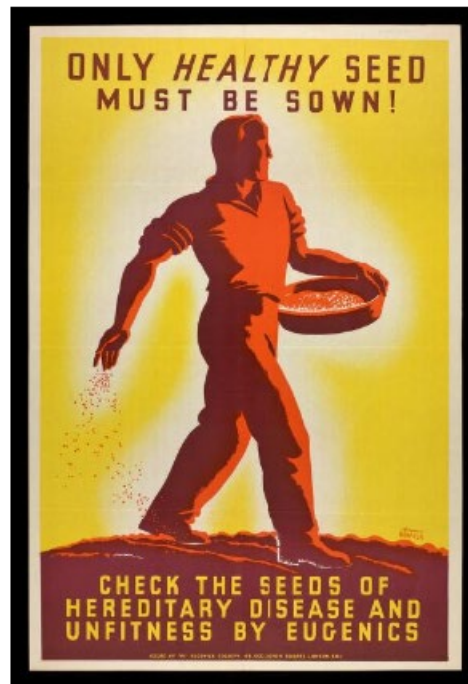


Figure 14: Wellcome Library, 2019[b]

Conversely, eugenics propaganda was released by the Eugenics Society to raise awareness of the movement and its emphasis on family planning. Overt propaganda that was released and attributable to an organisation played a crucial role in attempting to raise the awareness and likability of eugenics.

Many of the ideas surrounding scientific racial and ethnic inferiority, also known as eugenics, came from British and American authors and academics. Prominent 20<sup>th</sup>-century British eugenicists such as Robert Reid Rentoul took a strong stance on severing genetic ties with those deemed inferior in his book *Race Culture, Or, Race Suicide? A Plea for the Unborn*:

*The negro is seldom content with sexual intercourse with the white woman, but culminates his sexual furor by killing the woman, sometimes taking out her womb and eating it. If the United States of America people [sic] would cease to prostitute their high mental qualities and recognize this negro as a sexual pervert, it would reflect greater credit upon them; and if they would sterilize this mentally afflicted creature instead of torturing him, they would have a better right to pose as sound thinkers and social reformers (Rentoul, 1906, p.31-32).*

The significance of Rentoul's inflammatory remarks is both chilling and worthy of further inspection predominantly since chapter 3 displays a propaganda image created by the FBI that shared similar themes (see figure 21). During the FBI's psychological warfare crusade against the Black Panther Party, racially inflammatory cartoons were drawn and posted to panther members to incite racial tension between white and black citizens. As displayed in chapter 3, this propaganda theme was focused on the alleged obsession that black men, particularly Black Panther members, had with white women; a key theme that has survived multiple centuries.

Sterilization was a procedure that was used by eugenicists to prevent people from passing on alleged defective genetic traits to children who would allegedly grow up as *feebleminded* and contaminate healthier gene pools thus bringing down the genetic strength of a country. Albeit, Rentoul's views were extreme; he was not alone in his support for eugenics. In fact, according to Steven Farber:

*Many intellectuals and political leaders (e.g., Alexander Graham Bell, Winston Churchill, John Maynard Keynes, and Woodrow Wilson) accepted the notion that modern societies, as a matter of policy, should promote the improvement of the human race through various forms of governmental intervention. While initially this desire was manifested as the promotion of selective breeding, it ultimately contributed to the intellectual underpinnings of state-sponsored discrimination, forced sterilization, and genocide (Farber, 2008).*

Farber's assessment has proven to be logically and historically sound due to the nature in which eugenics evolved into the wholesale slaughter of Jews in Nazi Germany. However, before delving further into great detail about eugenics propaganda, it is vital to outline and define eugenics and its background. Charles Darwin's theory of *Evolution* outlined the process of how a species traits and capabilities mutate over time to survive the terrain that they inhabit (Darwin, 1859, p.80-86). Life becomes a battle of the fittest species that can evolve efficiently to prevent early death from predators or to survive a harsh terrain (Darwin, 1859, p.80-86). Weaker species or at least insufficient traits within a particular group will eventually die off, leaving only those who have evolved. Darwin's cousin, Francis Galton, took a liking to the notion that the fittest will survive the battle of life (Galton, 1907, p.307). Galton envisioned Darwin's theory of Evolution being applied to

human races and social classes (Galton, 1907, p.307). That is to say, the fittest race among humans would survive. In contrast, the weaker lower working class and darker races will be a burden to Anglo-Europeans and eventually be drastically curtailed or removed as the expansion of Anglo-Europeans continued throughout the *new world*.

As detailed in Galton's book *Inquiries Into Human Faculty and Its Development* that was published in 1883, Galton coined the term eugenics. Galton referred to the 'cultivation of race' as Eugenics (Galton, 1907, p. 24). Moreover, Galton hoped that by investigating *superior* beings, a methodology of breeding favourable people would produce a strong bloodline to advance society. In contrast, weaker lineages would be curtailed or managed; only having a marginal role and presence in society. Or put in another way, 'the most merciful form of what I ventured to call "eugenics" would consist in watching for the indications of superior strains or races, and in so favouring them that their progeny shall outnumber and gradually replace that of the old one' (Galton, 1907, p.307).

This standard of delineating fit from unfit became a landmark issue in the US Supreme Court during the case of *Buck v Bell* (in 1927) which eventually gave justification to forced sterilizations (Georgetown University, n.d.). Carrie Buck was a young woman who had been raped and subsequently gave birth to a child that was deemed to be an imbecile. Buck was assigned to a mental asylum called Virginia Colony by her foster parents after she gave birth. Buck's mother, Emma Buck was previously committed to the same asylum (University of Virginia, 2007). During this tumultuous period for Buck (Carrie), a sterilisation law was passed in Virginia, to which the state was authorised to support forced sterilisation of mental defectives to promote the 'individual health and welfare of society' (Justia, 2019[a]; National Archives and Records Administration (US) (2017[b])). At the climax of the *Buck v Bell* Supreme Court case, a chilling opinion handed down by Justice Oliver Wendell Holmes summarised America's attitude towards those it deemed socially inferior. Accordingly:

*It is better for all the world, if instead of waiting to execute degenerate offspring for crime, or to let them starve for their imbecility, society can prevent those who are manifestly unfit from continuing their kind. The principle that sustains compulsory vaccination is broad enough to cover cutting the Fallopian tubes. Three generations of imbeciles are enough* (Georgetown University, n.d.).

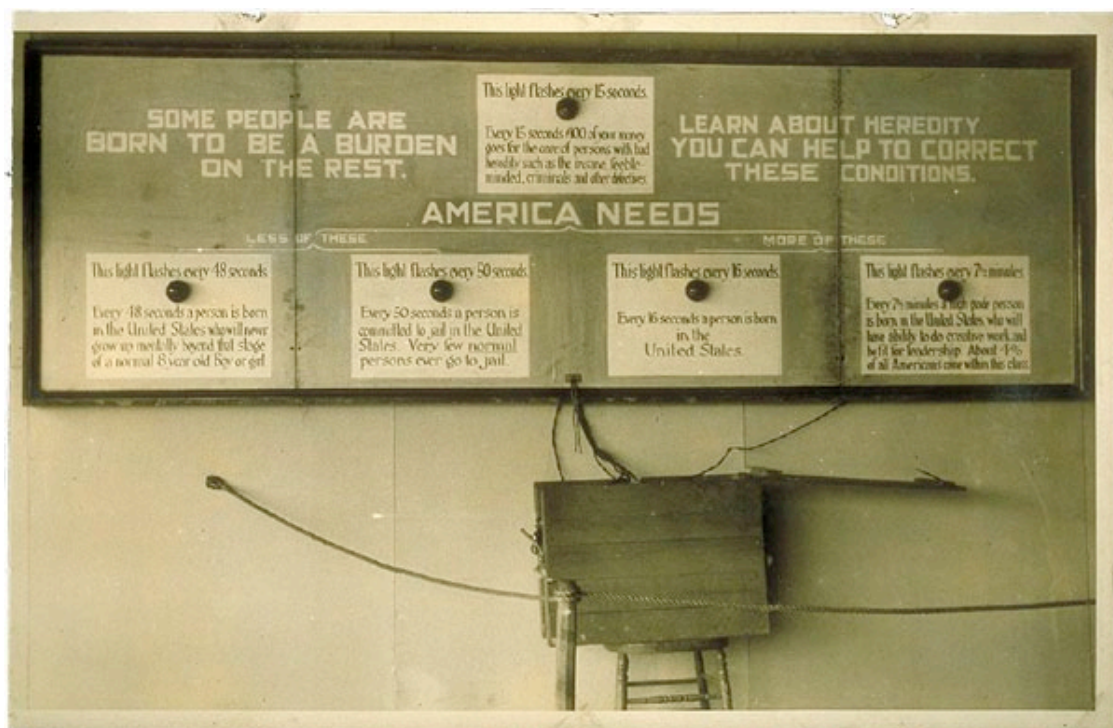
For such a crude approach to human life to exist without inciting the sense of cognitive dissonance or regret for humiliating innocent citizens, propaganda was required to reinforce the need to abide by eugenics and its legal ramifications discussed above. Supplanting dissonance with support for eugenics was partly fulfilled by eugenics exhibitions that acted as strategic information bases. Eugenics exhibitions helped convince Americans of the need to improve the overall gene pool of the nation. Black people in Africa and North America were targets of eugenics philosophy. In particular black features were dehumanised and made to look outlandish to the extent that questions were raised as to what extent black people could be referred to as fully human. Below in figure 15, Dr A.H. Schultz of the Carnegie Institution of Washington had compared the development of white and black foetuses, aiming to delineate and point to differences between the races (Cold Spring Harbor Laboratory, n.d.).



Cold Spring Harbor Laboratory. Noncommercial, educational use only.

Figure 15: Cold Spring Harbor Laboratory, n.d.

Moreover, eugenics exhibitions served as an integral base for propagandists to *educate* the public on the necessity of managing carefully who they reproduced with. Figure 16 reveals alleged statistics which suggest that every 18 seconds a person is born in the US in which due to his or her hereditary defilement will not "grow up mentally beyond that stage of an 8-year boy or girl" (Cold Spring Harbor Laboratory, 2019). Erroneous facts such as those displayed in figure 16 helped to ferment an atmosphere of resentment towards people such as Buck who were placed in asylums for being (allegedly) feeble-minded or mentally defective (Cold Spring Harbor Laboratory, 2019).



American Philosophical Society. Noncommercial, educational use only.

Figure 16: Cold Spring Harbor Laboratory, 2019

Overall, the US experience of eugenics was crude and widespread. Propaganda sought to ease the moral and religious dissonance that came from accepting that the bloodline of those deemed undesirable should be wiped out of existence or curtailed at the behest of voluntary or forced sterilisations. This thesis accentuates the extensive ability of covert un-attributable propaganda to deceive and manipulate people all over the world. Multiple chapters will reinforce and justify this claim. Conversely, it is of great importance to emphasise that overt propaganda which is attributable to a source, can asphyxiate the

moral conscience of an entire nation, much to the detriment of human rights and civilisation.

Germany, much like the UK and the US adopted the principles of eugenics. After WW1, Germany was devastated by its defeat to the Allies. Questions surrounding the social burdens to the state became amplified in an atmosphere of economic scarcity which even managed to penetrate the rationale of German Catholic priests (Dietrich, 1992, p. 577-580).

Admiration for eugenics throughout Europe manifested itself in propaganda posters and exhibitions that helped to display the need for cultural change in sexual and social practices. Eugenics propaganda emanating from Germany provided the necessary amount of persuasion to dispel any sense of dissonance or resistance to targeting its Jewish population, disabled and Roma inhabitants. Academics and researchers proved to be vital in creating and promulgating erroneous scientific claims which could be arguably classified as grey propaganda. In Germany, the measurement of skulls was a prominent modus operandi for legitimising propaganda emanating from the Third Reich towards its many targets (Berg, 2008 p.175). Academics such as Eva Justin, Robert Ritter and Joseph Mengele were a maligned intellectual nucleus that validated decisions to send Sinti and Roma people to be executed (Schuch, 2017, p. 609).

Research from Benjamin Madley has emphasised the role that Justin played, which highlighted that after she examined Gypsies, many of them were sterilized or murdered (2005, p.456). Justin took particular interest in investigating head shapes to reify prejudicial assessments that would likely lead to sterilization's or execution (see figure 17) (United States Holocaust Memorial Museum, n.d.). This flawed research method was predicated on previous German obsession with skulls of black African's that they had obtained during its pacification and colonisation of former German South-West Africa (Namibia). After comparing skull sizes between Europeans and Herrero and Nama inhabitants, German scientists concluded that Africans were an inferior race, which led to a wave of racist propaganda towards many targets that the Nazis would later make use of.



SS leader Heinrich Himmler in 1943 stated that ‘Anti-Semitism is exactly the same as delousing. Getting rid of lice is not a matter of ideology. It is a matter of cleanliness’ (Himmler 1943, cited in Stephens, 2019). In effect, the Nazi party utilised the language of its recent past and churned out propaganda lines that embodied a desire to keep Germany clean. According to Madley:

*Rationalize goals and methods that violated Christian morality and European martial norms, German leaders in both colonial Namibia and Eastern Europe deployed public health rhetoric. Although discussions of racial hygiene and eugenics were common in late nineteenth- and early twentieth-century Germany, these linguistic overlaps suggest that rhetoric associated with German [South-West] Africa was a source from which Nazis borrowed (Madley, 2005, p.445).*



Figure 17: United States Holocaust Memorial Museum, n.d.

From this angle, academic eugenics propaganda can be viewed as integral to speeding up or at least helping to ideologically facilitate and ferment the process of genocide in Nazi Germany and former German South-West Africa. In Nazi Germany, propaganda was particularly crude and set out to emphasise the necessity of keeping the German Aryan race pure. Multiple pictures, posters and actual displays of human skull sizes played a crucial role in keeping German nationalism alive and vigilant from external forces who opposed Hitler’s vision of a pure Aryan race. One particular example included a picture of an Aryan woman and a black woman smiling together as a social taboo that degrades racial pride (United States Holocaust Memorial Museum, 2017). As displayed in figure

18, the caption states "The experience/Racial pride fades" (United States Holocaust Memorial Museum, 2017).



Figure 18 United States Holocaust Memorial Museum, 2017

Furthermore, film propaganda was a useful tool that helped to depict in motion, those that Nazi Germany had cast out and left to languish due to their perceived mental defectiveness. Under Nazi Germany, the Office of Racial policy produced film propaganda from a mental hospital that sought to accentuate and bolster support for eugenics and social purity throughout the country. In doing so, Nazi Germany hoped to portray Jews and mentally challenged people as worthy of being cast out from society and if necessary, culled.

The term used to describe the people in this particular Nazi educational propaganda was "unheilbare Geistkranke" which translates as the incurably insane (see figure 19). Nazi propaganda sought to aggrandise social tension by incorrectly suggesting that those living in mental hospitals lived a life of "Luxury" while ordinary Germans struggled (United States Holocaust Memorial Museum, 2019). This form of reasoning accentuated the need to have a society based on strong working men that could restore Germany's pride having been defeated by the Allies in WW1.



Figure 19: United States Holocaust Memorial Museum, 2019

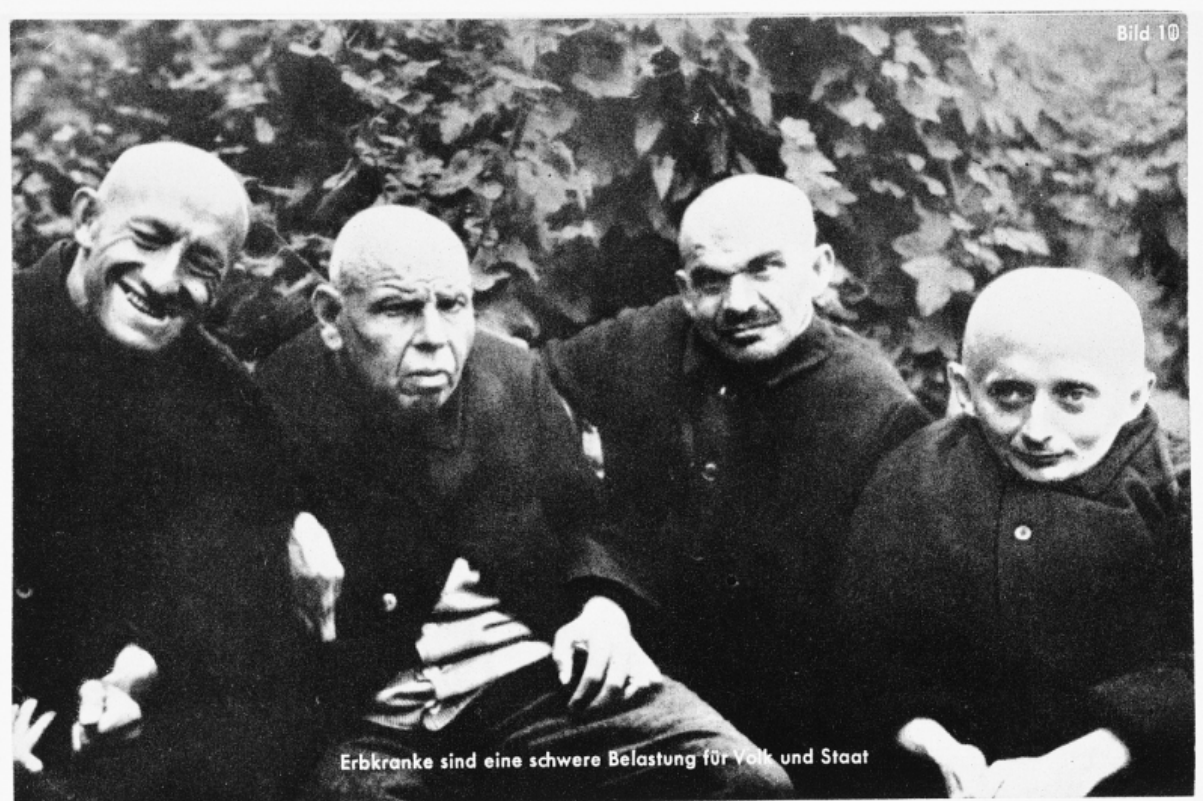


Figure 20: (United States Holocaust Memorial Museum, 2014)

Similarly, figure 20 displays four disabled men in a pejorative light. During Nazi rule, an estimated 275,000 disabled people were killed. The caption in figure 20 states that disabled people encompass a hereditary illness and are a “heavy burden for the people and the state” (United States Holocaust Memorial Museum, 2014). Propaganda does not need to be covert to get a particular point across to the masses of society. The openness of Nazi propaganda is particularly concerning because society was so willing to accept open discrimination. An attitude of nonchalance helps to breed atrocities that were experienced by multiple groups in Nazi Germany. Propaganda may not be as effective if a group of people or society itself is unfamiliar with certain talking points. Symbolism and various talking points need to be reinforced continually before crude images such as figure 20 are accepted as factual without much cognitive dissonance.

For this reason, propaganda is particularly dangerous to those who have already been radicalised or are open to insidious ideas. Chapter 6 covers this particular issue in detail

as the FBI targeted citizens with propaganda who were already curious about terrorism and encouraged them to commit acts of terrorism in Syria. Nazi Germany and eugenics propaganda are grotesque but relevant examples that demonstrate what propagandists are capable of inspiring in those who are already susceptible to cruel and outlandish ideas.

---

### 3.11 Cold War Propaganda

---

Post WW2 propaganda was seen as a necessary tool to win a new war without the need for direct physical confrontation with another great power. The battle for allegiance between Western capitalist states and the communist world was fought through proxy wars on an ideological basis. Ideology and loyalty to each side required reinforcement. During the mid-1940s, US policymakers feared the increase in popularity and party numbers of communist political organisations in Europe. In the case of Italy, the US made a concerted effort in the late 1940s to weaken communist political networks that were surfacing and inciting grave national security threats to the Italian De Gasperi government. A substantial amount of fear gripped the Italian and USG concerning the possibility that communist elements might attempt a coup or to gain power through elections (Office of the Historian, 1947). In 1947 a US memorandum by Samuel Reber, the acting director of the office of European Affairs, stated that:

*[C]ommunists have instigated intermittent work stoppages ... disorders... raided and wrecked rightist party headquarters and newspaper plants ... laid siege to prefectures and police stations and have attacked prisons seeking to release comrades arrested during the disorders (Office of the Historian, 1947).*

Towards the end of 1947, US NSC 1/1 was drafted because of concerns regarding Italy's future. Among a litany of commitments made to support Italy, the US declared that it would be '[a]ctively combatting communist propaganda in Italy by an effective US information program and by all other practicable means' (Office of the Historian, 1948[a]). In addition to the previous concerns cited regarding an uprising in Italy, Ranelagh has suggested that the former US Secretary of Defence James Forrestal was:

*[W]orried by the prospect of a communist or communist/ broad left victory in the forthcoming Italian elections, and he saw the CIA as offering a means of secretly influencing the elections in the interests of the democratic parties, in particular the Christian Democrats (Ranelagh, 1987, p.115).*

The US purportedly spent incredibly large sums of money on Italian elections. Research from former CIA agent Phillip Agee has highlighted that ‘The Pike committee...describes how the CIA has spent some \$75 million in Italian political campaigns since 1948, with \$10 million spent in the 1972 elections alone’ (House of Representatives (US), 1976, cited in Agee, 1978, p.267). US aid went to democratic anti-communist parties such as ‘the Christian Democrats, the Republican party (Partito Repubblicano Italiano, PRi), and the Social Democratic Party (Partito Socialdemocratico dei Lavoratori Italiani, PSLI)’ as a means of influencing the election in favour of the Democratic Parties (Del Pero, 2001, p.1306). Additionally, under the Truman administration in 1947, fears about Soviet international propaganda campaigns startled the NSC, which led to the authorisation of foreign covert warfare. The NSC 4-A enabled US covert operations overseas (Office of the Historian, n.d.[b]). According to the NSC 4 document:

*The USSR is conducting an intensive propaganda campaign directed primarily against the US and is employing coordinated psychological, political and economic measures designed to undermine non-Communist elements in all countries. The ultimate objective of this campaign is not merely to undermine the prestige of the US and the effectiveness of its national policy but to weaken and divide world opinion to a point where effective opposition to Soviet designs is no longer attainable by political, economic or military means (US Department of State, 2001).*

To remedy the alarming situation that Washington found itself in, NSC 4 indicated that the world required strengthening and assistance designed to influence attitudes globally (US Department of State, 2001). Such measures to counter Soviet psychological warfare, were to be conducted by the CIA (US Department of State, 2001). In general, US psychological warfare plans included:

*[S]abotage, anti – sabotage, demolition and evacuation measures; subversion against hostile states, including assistance to underground resistance movements, guerrillas and refugee liberation groups, and support of indigenous anti-Communist elements in threatened countries of the free world (Office of the Historian, 1948[b]).*

Synonyms or offshoots of psychological warfare such as political warfare were viewed as necessary and rational by prominent state figures such as Kennan (in 1948), due to the increasing threat of Soviet psychological warfare (Wilson Center, 1948, p.2). In the view of Kennan:

*[P]olitical warfare is the employment of all the means at a nation's command, short of war, to achieve its national objectives, to further its influence and authority and to weaken those of its adversaries. Such operations are both overt and covert. They range from such overt actions as political alliances, economic measures (as ERP), and “white” propaganda to such covert operations as clandestinely support of “friendly” foreign elements, “black” psychological warfare and even encouragement of [u]nderground resistance in hostile states (Wilson Center, 1948, p.2).*

What is most striking from Kennan’s perception of influencing other states is that there was a genuine perception from policymakers that the US had ‘assumed greater international responsibilities than ever before’ to counter Moscow quite literally wherever the communist trail was located (Wilson Center, 1948, p.3). Also, it is essential to note that the US endeavoured to drastically curtail Soviet influence, as opposed to attempting to overthrow the Soviet Union. In 1952, the NSC 10/5 cited its previous NSC 20/1 in stating that:

*This strategy, however, as is most explicitly stated in NSC 20/1, does not include efforts “to bring about the overthrow of the Soviet Government”... “It is idle to imagine” that the achievement of objectives involving such issues” could be brought about by means short of war”... The general strategy for [C]old [W]ar operations under 10/5 must therefore be designed to contribute to the retraction*

*and reduction of Soviet power and influence by methods short of war and without the overthrow of the Soviet Government (CIA, 2016[c], p.2).*

Cognisant of America's self-proclaimed lack of maturity in the field of psychological warfare, the NSC 10/5 accepted that it might take some time before significant or desirable results in covert capabilities manifest (CIA, 2016[c], p.3). However, this did not stop Washington from trying to agitate the social geopolitical structures of the Soviet Union. In East Berlin and other Soviet satellite European states, elements of dissent and unrest were beginning to surface early on during the Cold War. Blessed with a self-prescribed international remit, US intelligence drafted plans to intervene and create psychological effects to favour American interests in Europe (National security Archive (US), 1953[a], p.2). In 1953 NSC 158 explored measures that could be taken against the unrest that engulfed Eastern Europe. The objectives that were set out included:

*[N]ourishing resistance to communist oppression throughout satellite Europe, short of mass rebellion in areas under Soviet military control, and without compromising its spontaneous nature... To exploit satellite unrest as demonstrable proof that the Soviet Empire is beginning to crumble (National security Archive (US), 1953[a], p.2).*

East Germany, in particular, was a target of psychological exploitation during riots that ensued. As put by John M. Anspacher in a memorandum to George Morgan, those that were shot by Soviet soldiers during the unrest should be made a martyr throughout the world, to shatter the idea of Soviet-backed unity (National Security Archive (US), 1953[b], p.2). This was a part of a broader plan to accentuate America's support for a unified Germany and to launch psychological warfare tactics such as covert radio broadcasts (National security Archive (US), 1953[a], p.3). Overall, a key theme to take from the American experience was its self-prescribed remit to engage in propaganda campaigns throughout Europe. This is a central theme in Chapter 8 in which the US began distributing grey and black propaganda in Iraq.



---

## 3.12 The IRD anti-Communist propaganda: From Nigeria to Latin America

---

Intelligence services such as the IRD played a vital role in shaping perception at home and in foreign countries in which communist subversion was a potential or real threat. The UK was concerned about the fate of one of its former colonial possessions, which was at risk of being influenced by communism. Colonial and post-colonial Nigeria was imbued with a series of tribal and political issues, particularly during elections. The Foreign Office and the IRD saw this as an opportunity for communists to fan the flames within Nigeria and make her become ‘the target of more sustained attacks and possibly active subversion by the more extreme African states, probably led by Ghana’ (TNA (UK): FO 1110/1961). To negate any communist ideation by the Nigerian public, the UK Foreign Office and the IRD sought to launch a covert information campaign in Nigeria through various local (Nigerian) accomplices. In a letter sent by the Colonial Office in 1956, it was stressed that:

*The material in question is a series of pamphlets, booklets... produced by a branch of the Foreign Office known for cover reasons as Information Research Department or “I.R.D.”, which is a sizable organisation and is financed at least in part from secret funds. Their concern is precisely to provide counter-propaganda material and to busy themselves with the direct countering of Communist efforts overseas (TNA: CO 1035/117).*

At times Britain sought to distribute books that were genuinely published by real authors. However, such books were anti-communist and highlighted contentious points within communism. According to a Foreign and Commonwealth Office letter concerning the supply of IRD material to Nigeria, ‘St. Elmo Nelson’ had made requests for ‘for books on Islam in the Soviet Union’ (TNA (UK): FCO 95/971). Moreover, much like the OSS strategy of avoiding mass communication, Britain’s strategy to counter communist propaganda in Nigeria aimed to place its content in the hands of influencers who could help to crystallise public opinion. This did not mean that Britain avoided introducing a significant amount of propaganda in Nigeria but that they were aware of the need to

influence the influencers. Highlighted by the Foreign Office concerning the scope of IRD work in Nigeria:

*As I see it at the moment, IRD work here can be most effective... in providing the more sophisticated background material on Communism to the relatively small range of people, college principals, lecturers, writers, editors etc., who can be regarded as moulders of public opinion (TNA (UK): FO 1110/1961).*

A testament to this claim is the fact that co-operation of the British Information Service led to ‘increasing amounts of IRD material... being accepted by the press in Lagos’ (TNA (UK): FO 1110/1961). In northern Nigeria, distribution of IRD information was extensive and included contacts of Nigerians who had prestigious positions in academia, the military and the police. For example, the following is a list of names and positions that were to receive IRD material in northern Nigeria:

*Alhaji A.L. Umaru – secretary to the military government... Mr. J.K. Salihu – Chief Inspector of Education, Ministry of Education... Mr.J.O. Popoola Librarian, Kwara State Library... Professor J. O’ Connell – Head of faculty of Government, Ahmadu Bello University... Mallam Yakubu Adamu – Advanced Teachers’ Training College... Mr. J.E. Freeman Permanent Secretary, Ministry of Education, jobs... Alhaji Abdullahi Abubakar – Chief Information officer, Military Governor’s Office, Maiduguri (TNA (UK): FCO 95/971).*

Overall, Britain aimed to steer its former colonial possession in a direction that suited its (British) geopolitical orientation. Although Nigeria was set free from the yoke of British colonialism, in theory, declassified material shows that Nigeria’s citizens were not free to decide crucial domestic issues without intervention from IRD and the Foreign Office.

---

### 3.13 The IRD in Latin America

---

Since the Monroe Doctrine and successive US interventions in Cuba, Haiti, Nicaragua and The Dominican Republic and Latin America in general, was viewed as America's sphere of influence. After the fall of the Batista regime in Cuba at the hands of Fidel Castro, the UK had become concerned about the regional, ideological posture of Caribbean nations. Conscious of the fact that Castro had successfully overthrown a US-backed ally (Batista) from power, in the eyes of the UK Foreign Office, the Castro regime represented a prototype for socialist revolution in the region (TNA (UK): FO 1110/1561). A vast amount of declassified information has shone a light on Britain's stance towards communist activity in the region, and the means with which she responded to the threat. During the early 1960s, the Foreign Office took the view that:

*Until comparatively recently, Latin America has not been regarded as a priority target for the United Kingdom information effort. Politically, the area seemed relatively sheltered from the major storms of world affairs...This situation has now radically altered. Vastly improved media of communication have brought home to the masses as never before the issues now being fought out in every field of human activity between the Communist camp and the free world... Her Majesty's Government, like other Western powers, are therefore actively reconsidering their information effort towards the area (TNA (UK): FO 1110/1561).*

London, made additional financial provisions to bolster its information effort in Latin America, spending an extra £170, 000 from 1960 to 1962 (TNA (UK): FO 1110/1561). To no surprise, in 1962 the IRD's endeavours were extensive in scale. One particular IRD project envisaged 'the distribution of 100,000 copies of a booklet' in Latin America to help dampen socialist ideation in the region (TNA (UK): FO 1110/1561). As was the case in Nigeria, media outlets that could warp perception of the masses were targeted and used by the IRD to place favourable information in Latin America. In 1949, a Foreign Office letter highlighted the significant steps taken to counter communism in Brazil:

*Some satisfactory developments achieved recently in the dissemination here of the material – anti-communist – produced by the Information Research Department... Some months ago my Information Officer, Stow, took the Director of the Brazilian Government Information Agency into his confidence, and arranged with him for I.R.D. material to be distributed through the Agency's press service for the Interior. In this way our stuff now goes to approximately 170 newspapers in the interior of the country. It is in the interior that Government fear most the spread of Communism, since the workers there are less under the influence of the Government – controlled workers syndicates (TNA (UK): FO 1110/182).*

In other nations such as Colombia, a total of 190 booklets were distributed from 1969-1970 (TNA (UK): FCO 95/979). A whole host of figures and institutions were targeted in Colombia, including, '[g]overnment officials...Political parties...Armed services...Editors Journalists...writers, Religious leaders' (TNA (UK): FCO 95/979).

Moreover, after Fidel Castro took power in Cuba, British intelligence began to target the regime with non-attributable propaganda. The Foreign Office policy at the time was to ensure that, '[t]he Information Research Department, the Regional Servicing Centre at Mexico and the Regional Information Officer at Caracas' was to work towards increasing 'the supply of non-attributable material critical of the Castro regime' (TNA (UK): FO 1110/1561).

Furthermore, it is important to highlight that British covert information campaigns in Latin America also manifested in the form of radio propaganda. In direct response to the communist threat in Latin America, one declassified document asserts that '[t]he regional servicing Centre... has recently initiated the production of radio tapes in Spanish based on ...IRD material and these are now being broadcast in 12 countries' (TNA (UK): FO 1110/1561). Overall, the IRD sought to capitalise on un-attributable propaganda in Latin America to counter the ideological spread of communism. In light of the fact that the UK had post-colonial links with various countries in the Caribbean, it was desirable to prevent the rise of communism to protect trade links and strategic spheres of influence.

---

### 3.14 The CIA in Latin America

---

In contrast to Britain's information approach in Latin America, the US pursued a more aggressive policy within Latin America. As previously mentioned, the US considered Latin America to be America's sphere of influence throughout the 20<sup>th</sup> century. Early in the Cold War, President Jacobo Arbenz of Guatemala fell out of favour with Washington due to his pursuit of nationalist policies. President Arbenz's policies prompted the CIA to take action in the form of a coup in favour of 'a disgruntled general named Carlos Castillo Armas' (National Security Archive (US), 2017). In 1953 President Eisenhower authorised operation PBSUCCESS to overthrow President Arbenz, which was reinforced by 'a \$2.7 million budget for "psychological warfare and political action" and "subversion," among the other components of a small paramilitary war' (National Security Archive (US), 2017). The psychological aspect of the CIA's covert action, codenamed Operation Sherwood, played a vital role in placing President Arbenz's administration under a considerable amount of pressure (Cullather, 1997, p.63; National Security Archive (US), 2017).

Coups are usually associated with displays of force on the streets by opposition elements. However, a CIA memo designated for Eisenhower states that the endeavour against President Arbenz relied 'on psychological impact rather than actual military strength' (Office of the Historian, 1954). Radio propaganda was used to create an atmosphere of hostility in Guatemala. According to one CIA document, '[a] clandestine radio broadcasting station was established in Nicaragua. The purpose of these broadcasts was to intimidate members of the communist party and public officials who were sympathetic to the communist cause' (Office of the Historian, 1975).

As previously discussed with regards to the British experience of covert propaganda, planting information was an essential method for Washington to sway perception in Latin America. In the case of the Guatemalan coup, CIA collaborators in conjunction with skewed media reports helped to ferment worry and dissent. At the time of the coup, '[o]ne of the propaganda ploys was to fabricate reports of Soviet arms deliveries to Guatemala by submarine, and then arranging to have a CIA planted cache of Soviet arms discovered and publicized' (Office of the Historian, 1975). The CIA's psychological ploy was

designed to exhibit the necessity of rejecting communism and the Soviet Union that were (allegedly) sponsoring aggressive acts of subversion against democratic governments. Furthermore, in direct contrast to the CIA's outrage and disgust at the Soviet Union's forgery campaign discussed in Chapter 7, Historian William Blum uncovers similar tactics used by the CIA in Peru. According to Blum:

*A commando raid by anti-Castro Cubans upon the Cuban embassy in Lima had uncovered documentary proof that Cuba had paid out "hundreds of thousands" of dollars in Peru for propaganda to foster favourable attitudes toward the Cuban revolution and to promote Communist activities within the country (Blum, 2003, p.172).*

However, it turned out that some of the documents were not authentic. Former CIA Officer Agee has stated the:

*The Lima station inserted among the authentic documents several that had been forged by TSD [Technical Service Division] including a supposed list of persons in Peru who received payments from the Cuban Embassy totalling about 15,000 dollars monthly. Another of the forged documents referred to a non-existent campaign of the Cuban Embassy in Lima to promote the Ecuadorean position on the Rio Protocol (Agee, 1975, p.121).*

To begin with, the forgery did not gather momentum among Peruvians; therefore this scandal struggled to the desired level of ferment media attention and public outrage in a manner that would hurt Cuba's reputation (Agee, 1975, p.121). However, with the compliance of a former Cuban embassy defector that cooperated with the CIA in order to confirm the authenticity of the fake documents; eventually, the Peruvian government decided to break diplomatic relations with Cuba (Agee, 1975, p.121). The so-called scandal eventually appeared in the Lima press as a means of warping perception in Peru (Agee, 1975, p.121).

Moreover, after Jose Velasco had come to power in Ecuador in 1960, the CIA became concerned about his reluctance to break ties with Cuba. Consequently, the CIA engaged

in what Blum has referred to as a 'textbook of dirty tricks' (1986, p.170). In addition, Blum has suggested that:

*Throughout most of Latin America, the Agency planted phoney anti-communist news items in co-operating newspapers. These items would then be picked up by other CIA stations in Latin America and disseminated through a CIA-owned news agency, a CIA-owned radio station, or through countless Journalists being paid on a piece-work basis, in addition to the item being picked unwittingly by other media, including those in the United States. Anti-Communist propaganda and news distortion (often of the most farfetched variety) written in CIA offices would also appear in Latin American newspapers as unsigned editorials of the papers themselves (2003, p.154).*

Planting information in news sources was of great importance to the CIA's information war against communism and its advocates in the Soviet Union. Unwitting civilians would consume this information without knowledge of the CIA's hand, therefore, making it an ideal tactic to operationalise. Additionally, as the CIA's efforts against Velasco intensified, the Agency made use of a slightly different form of propaganda. The Agency began creating organisations that pushed anti-communist propaganda. According to Blum:

*If, at a point in time, there was no organization that appeared well-suited to serve a particular need, then one would be created. Or a new group of "concerned citizens" would appear, fronted with noted personalities, which might place a series of notices in leading newspapers denouncing the penetration of the government by the extreme left and demanding a break with Cuba. Or one of the noted personalities would deliver a speech prepared by the CIA, and then a newspaper editor, or a well-known columnist, would praise it, both gentlemen being on the CIA payroll (1986, p.171).*

Similarly, staged psychological warfare was a tactic that was used by the CIA to shape perception in Latin America. According to Agee:

*[A] timely bombing by a station agent, followed by mass demonstrations and finally by intervention by military leaders in the name of the restoration of order*

*and national unity, is a useful course. Agency political operations were largely responsible for coups after this pattern in Iran in 1953 and in the Sudan in 1958 (Agee, 1975, p.64).*

In a similar light, Blum suggested that the CIA was responsible for church bombings in Ecuador. During the campaign against Velasco:

*'CIA agents would bomb churches or right-wing organisations and make it appear to be the work of leftists. They would march in left-wing parades displaying signs and shouting slogans of a very provocative anti-military nature, designed to antagonise the armed forces and hasten a coup' (Blum, 2003, p.173).*

Attribution is a prominent theme in the CIA's attempts to blame someone else for a nefarious act. Chapter 6 revolves around the democratic proselytisation of terror in which the FBI created a fake terrorist website to attract followers. It would appear that misattribution is a running theme in America's propaganda ethos.

---

### **3.15 COINTELPRO, Black Nationalists and the FBI's Propaganda**

---

Throughout the Civil rights period, the US became concerned about the rise of black nationalist ideation within the African American community. Similarly, the FBI, in particular, became fearful of prominent figures such as MLK with regards to his influence among African Americans and his public attacks on the USG's war in Vietnam. MLK's 1967 *Beyond Vietnam* speech convinced the FBI that he had fallen under the influence of communists, subsequently leading to an increase in surveillance towards MLK (Stanford University, n.d.).

After the assassination of MLK, the FBI continued its surveillance and information campaigns against groups it categorised as *Black Extremists*. To counter the threat of black figures that the FBI feared, the bureau's COINTELPRO sought to infiltrate, disrupt and in the case of the Black Panthers work towards 'decimating the Party's leadership' (National Archives and Records Administration (US), 2019). Black nationalists from the



Memphis group called the Invaders were subject to daily articles that revolved around derogatory leaked information about previous financial crimes (FBI, 1968[b], p.16). The FBI concluded that exposure of extortion had resulted in the Invaders being portrayed as ‘young thugs preying on their own race’ (FBI, 1968[b], p.16). Much like the Morale Operations that were orchestrated by the OSS during WW2, the FBI crafted anonymous letters to be sent to Black Panther members in Detroit. According to a memorandum dated in 1969, ‘[t]his letter will be signed “A Concerned Sister” with the expectation that it will cause suspicion of Detroit BPP leader’ (FBI, 1969, p.8). This particular letter consisted of disruptive narratives designed to stir up friction amongst Black Panther Party members. One specific anonymous letter that was created by the FBI to stir confusion and animosity among followers of the Black Panthers went on to state the following:

*Dear brothers and sisters: who's next? You, me, who knows. Do you really believe brother Baynham blew his brains out...Was this ‘suicide’ and the ‘mercy killing’ of one of our other brothers in New Haven arranged by Chief Executioner Hilliard. Why doesn't chief brother Hilliard speak out on our lost brothers[?]* (FBI, 1969, p.8).

Also, the FBI noted that ‘[c]opies of this letter will be sent to leaders and members who would be most susceptible, based on intelligence data received from Detroit sources’ (1969, p.9). Propaganda and surveillance thus go hand in hand, as the latter helps to finesse the former. The internal division within the Black Panther Party was one of many reasons why the group gradually lost its appeal and eventually disintegrated. How much of this can be attributed to the FBI’s psychological warfare tactics is debatable, but this anonymous letter is indicative of the pressure that the Black Panther Party was put under.

Moreover, inflammatory cartoons were used by the FBI to exacerbate the ideological schism amongst black nationalists. FBI cartoons displayed Black Panthers with racially charged themes such as the notion that black men are sexually infatuated with white women and being in cahoots with white liberals. This was done to exploit racist tropes and slogans, e.g. *Uncle Tom* that orientated around the notion of African Americans abandoning *the black cause* to be in a better position within white America. In a communication sent by the FBI in 1969, permission was granted to mail copies of cartoons along to Black Panther members in Chicago. According to the FBI:

*Chicago has prepared three cartoons which are entitled "The taming of the Panther." "The Black Panther – House cat for the white the liberals" and "Follow Me." The first cartoon portrays a member of the Student for a Democratic Society (SDS) taming a wild Panther with a whip. The second cartoon portrays a white leftist with a black panther as a house cat (FBI, 1969, p.48).*

Such methods and themes endeavoured to cause friction between the Black Panther members, those deemed as white liberals and other groups within the civil rights struggle. In another case, the FBI terminated the following cartoon (see figure 21) for fear of its effectiveness. The unflattering portrayal illuminates the extent to which the USG was willing to traverse to shame black nationalists into submission.



Figure 21: FBI 1969, p.37

---

## 3.16 Cyber Propaganda in the 21<sup>st</sup> Century

---

In the age of information, intelligence services have attempted to keep a lid on the extent to which targets can influence perception in cyberspace. Put succinctly; intelligence services wish to reshape the power equilibrium in their favour. In particular, JTRIG have demonstrated the means and desire to control the perception of information on the Internet. Within Snowden's volume of leaks was a list of JTRIG tools and techniques for warping perception online. For example, a tool called GATEWAY can 'artificially increase traffic to a Web site' (EFF, 2014[c], p.5). Another technique, SLIPSTREAM, can 'inflate page views on Web sites' (EFF, 2014[c], p.6). Lastly, UNDERPASS can '[c]hange outcome of online polls' (EFF, 2014[c], p.6). These are remarkable cyber capabilities, as they possess the ability to alter information to which a potentially large amount of people will view. Online polls are conducted by a multitude of organisations throughout the world. Therefore, GCHQ has the capacity to pose a great risk to Internet users.

---

## 3.17 Digital Geneva Convention: Anarchy and State/Non-State Surveillance Ambitions in Cyberspace.

---

As the Second WW2 drew to an end, leaders from around the world were concerned about future conflicts. The UN was created to restrain interstate hostilities and forge an atmosphere of peace and prosperity. The UN Charter sets out to:

*To maintain international peace and security, and to that end: to take effective collective measures for the prevention and removal of threats to the peace, and for the suppression of acts of aggression or other breaches of the peace, and to bring about by peaceful means, and in conformity with the principles of justice and international law, adjustment or settlement of international disputes or situations which might lead to a breach of the peace (UN, n.d.[d]).*

International cooperation sought to combine efforts via the goals and principles set out in the UN charter to steer nations away from war collectively and to 'unite... strength to maintain international peace and security' (UN, n.d.[d]). Albeit noble, one contentious

assumption made during the creation of the UN and even up till this very date is that this international body can effectively deter selfish state ambitions while quelling existential risks and state anxieties. Much like the UN's predecessor, the League of Nations, effectively controlling states that undermine the principles of the body proved to be complicated. Economic, social, military and political manoeuvres within the international arena contorted the orderly and benevolent beliefs written on paper. Subsequently, the UN's authority was open to interpretation. Within a short period, nations from around the world took part in the Korean War from 1950 to 1953.

Surveillance, a key enabler of war and national security, is an age-old practice that the UN has struggled to effectively police. Moreover, in the contemporary cyber domain, the UN's ability to deter states from engaging in intrusive surveillance has become increasingly fraught with the Realist concept of anarchy and the overall infringement of privacy. In 1966, the International Covenant on Civil and Political Rights, which has been signed by 173 states, mandated in article 17 that '[n]o one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence' (OHCHR, 2019[a]). Decades later in 2013 'the United Nations General Assembly adopted resolution 68/167, which expressed deep concern at the negative impact that surveillance and interception of communications may have on human rights' (OHCHR, 2018[a]).

Despite UN resolution 68/167, during 2017 the OHCHR rightfully lambasted the actions of Western governments. As such the OHCHR stated that '[t]here is little or no evidence to persuade me of either the efficacy or the proportionality of some of the extremely intrusive measures that have been introduced by new surveillance laws in France, Germany, the UK and the USA' (2018[b]). Unfortunately, no matter how many kind words which may soothe the heart of listeners, stopping GCHQ's technological advancements that have undermined encryption standards will be difficult (EFF, 2014[d], p.2-4). Moreover, quantum computers have created fears of a 'crypto-apocalypse' in cyberspace due to the ease at which such a contraption will have at undermining current encryption standards (Office for Science (UK), 2016, p.50).

Considering how integral intelligence operations are to the state, in conjunction with how easy it can be for some intelligence services to steal information in cyberspace with relative impunity, cyberspace has descended into anarchy. This does not mean that every

state is equally throwing cyberspace into disarray. Seen as cyberspace and the field of intelligence is such a secret domain, knowing for sure the true extent to which all 191 + countries are or are not undermining cyberspace with intrusive surveillance and malware is difficult. In one sense, the famous proverb of, *if a tree falls in a forest and no ones there to hear it does it make a sound?*; sums up the difficulty of tracking hidden malware in cyberspace. If an intelligence service have hidden malware inside the network of an adversary or an ally and no one ever finds out, cyberspace is not as anarchic as it could be.

Moreover, the purpose of this chapter is to demonstrate with contemporary examples of how cyberspace has become an anarchic domain that cannot be unequivocally tamed by international cooperation. Furthermore, the concept of cyber stability will be used to assess the ability of the UN or a futuristic DGC to stem the appetite of intelligence services to subvert the network security of foreign nations. Also, this chapter will demonstrate how non-state actors such as the UN are incapable of bringing order in cyberspace.

Building a case to highlight anarchy in cyberspace will be done by exploring the British government's use of EI. Additionally, this section will focus on the use of leaked Snowden documents that highlight the NSA's expansive ambitions to undermine international encryption standards. Open source documents will also be used to help build this case. This will be juxtaposed with Smiths vision of a DGC (Smith, 2017[a]). This chapter is vital, as it sets the theme for the following chapters with regards to how and why propaganda and surveillance have become such a contentious issue in a realm in which no one can effectively police.

---

## 3.18 The Digital Geneva Convention

---

So far, a litany of aggressive and deceitful instances have been divulged. Considering the lack of cyber stability in contemporary times, the UN, G7, Smith and others have called for experts and governments to create a convention to recognise the fundamental rights of citizens in cyberspace as a means of ushering in an age of stability. G7 leaders have expressed concern ‘about the risk of escalation and retaliation in cyberspace’ which ‘could have a destabilising effect on international peace and security’ (G7, 2017, p.1). In light of this, G7 leaders ‘reaffirm that the same rights that people have offline must also be protected online and reaffirm the applicability of international human rights law in cyberspace, including the UN Charter, customary international law and relevant treaties’ (G7, 2017, p.2).

Similarly, the UN has also recognised that many countries are developing ‘ICT capabilities for military purposes. The use of ICTs in future conflicts between [s]tates is becoming more likely’ (Lewis, 2015). The desired counter to this would be to ‘identify further voluntary, non-binding norms for responsible State behaviour, and to strengthen common understandings in order to increase stability and security in the global ICT environment’ (Lewis, 2015).

Furthermore, recent revelations concerning the NSA’s stockpiled cyber vulnerabilities encouraged Smith to publicly call for states to ‘adhere in cyberspace to the same rules applied to weapons in the physical world. We need governments to consider the damage to civilians that comes from hoarding these vulnerabilities and the use of these exploits’ (2017[a]). The risk posed by state hacking and stockpiling of vulnerabilities compelled Smith to speak out and suggest that the world requires a global DGC to govern these issues, including a new requirement for governments to report vulnerabilities rather than to exploit them (2017[b]). In essence, Smith would like all of the protection people receive under international law to be applied to cyberspace to protect Internet users (2017[b]).

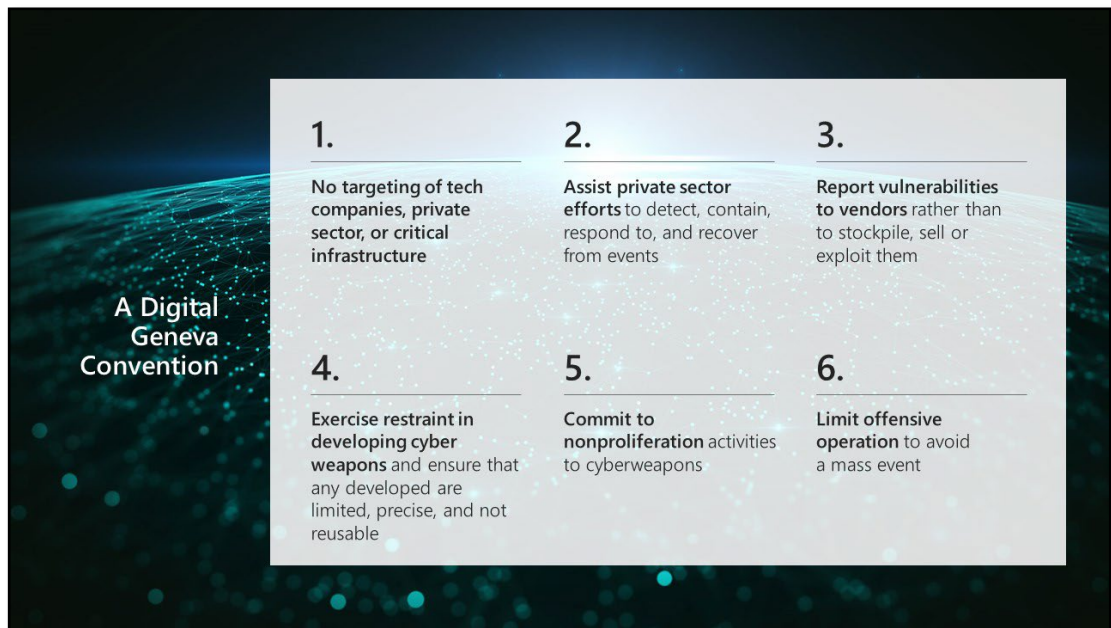


Figure 22: Smith, 2017[b]

A DGC would require ‘governments to come together, affirm international cybersecurity norms that have emerged in recent years, adopt new and binding rules’ (Smith, 2017[b]). This resonates significantly with Kant’s depiction of inter-state cohesion, to which he stated that *‘the greatest problem for the human species, whose solution nature compels it to seek, is to achieve a universal civil society administered in accord with the right’* (1983, p.33). Also, an independent body comprising of both public and private sector would be required to preside over such a convention ‘in a manner like the role played by the International Atomic Energy Agency in the field of nuclear non-proliferation’ (Smith, 2017[b]).

The DGC would require ‘an independent organization that can investigate and share publicly the evidence that attributes nation-state attacks to specific countries’ in the event of a violation (Smith, 2017[b]). Overall, such an idea would resonate with liberal or pluralist notions that ‘[d]emocratic processes and institutions would break the power of the ruling elites and curb their propensity for violence’ (Burchill, 2013, p.61).

Conversely, while the notion of a DGC is noble and without a doubt required, as Edward Carr eloquently highlighted ‘rationalism can create a utopia, but cannot make it real’ (2016, p.29). The first cracks in liberal notions appear to be directly projected by liberals

themselves. Beginning with the G7, a joint policy paper conceded to the fact that retaliation in certain circumstances might be necessary:

*We note that, in the interest of conflict prevention and peaceful settlement of disputes, international law also provides a framework for States' responses to wrongful acts that do not amount to an armed attack - these may include malicious cyber activities. Among other lawful responses, a State that is the victim of an internationally wrongful act may, in certain circumstances, resort to proportionate countermeasures, including measures conducted via ICTs, against the State responsible for the wrongful act in order to cause the responsible State to comply with its international obligations... We also recognized that States may exercise their inherent right of individual or collective self-defence as recognized in Article 51 of the United Nations Charter and in accordance with international law (G7, 2017, p.2 - 3).*

Until a single body or international agreement can constrain retaliatory attacks, cyberspace will suffer from the same ills that the physical world has been battling for thousands of years. Despite the liberal shell that G7 suggestions manifest in, the right of a nation to take matters into their own hands is still a crucial stumbling block within IR and cyberspace. According to article 51 of the UN Charter '[n]othing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations' (UN, n.d.[d]). How would Smith go about nullifying the UN Charter and a nation's right to defend itself in cyberspace for the sake of a pacifist orientated DGC?

This is where the concept of a DGC that prohibits retaliation begins to wane. States require EI to exfiltrate large and sensitive amounts of information. Although HUMINT still exists, cyber espionage is an incredibly valuable form of intelligence gathering. To put this into context, the British government constructed a hypothetical national security example of Biological Warfare (BW) capabilities that would require EI as a matter of self-defence against a hostile state:



*A hypothetical totalitarian state has an indigenous email system which is mandated for use by the general population, but also by scientists working on the state's biological weapons programme who are involved in the proliferation of weapons technology. This means it is used by many thousands of people within that country. The security and intelligence agencies can only obtain limited data from interception which means it is not possible to identify particular accounts which belong to individuals of intelligence interest working on the biological weapons programme. Bulk EI techniques would be needed to access a limited amount of data relating to a very large number of users of the service – potentially even all its users. This would enable the security and intelligence agencies to filter out those who were not of intelligence interest, and focus on those who were associated with the biological weapons programme in order to use targeted EI techniques against them to support the UK's aim of disrupting their proliferation of biological weapons (House of Commons, 2015[d], p.36).*

From this angle, states must act in a preponderant manner to ensure that they can keep track of hostile actors that may be developing weapons in secret, beyond the reach of the international community. GCHQ is one of the most advanced intelligence services in the world; therefore the British government may feel compelled to act in cyberspace to observe the behaviour of hostile actors when other forms of intelligence have not produced results. Historically, powerful states attempted to justify aggressive amoral behaviour in terms of responsibility to do right.

Ironically British Colonialism was in part based on fictional liberal notions of civilisation. Britain had the means and the resources to make a change within its imperium under the self-prescribed *white man's burden* or 'white imperial benevolence ...propaganda' which served to 'justify the colonies' (Easterly, 2006, p.245). However, when similar notions of responsibility based on capability manifest in cyberspace, many nations will feel it is their responsibility to follow up on intelligence leads and hack foreign countries, only this time for the sake of democracy instead of racial burdens. Without an overarching power that can decide what EI is justified, states will act preponderantly in cyberspace to deter external threats. Moreover, how would an already divided international body begin to cooperate when voting on amendments to the DGC if states already have vested interests in the physical world?

As maintained by the UN, Article 39 of the UN Charter states that:

*The Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decide what measures shall be taken in accordance with Articles 41 and 42, to maintain or restore international peace and security* (UN, n.d.[d]).

In the case of the UK, a threat could be coming from a hostile country that is an ally of another nation which has the power to veto UN motions that would investigate grievances. In recent events ‘the United Nations Security Council... failed to adopt a resolution on the mandate of an international panel investigating [the] use of chemical weapons in Syria due to a negative vote by permanent member, Russia’ (UN News, 2017). As a result, EI provides a viable solution to freely investigate and protect the UK and foreign allies from existential threats outside the yoke of international agreements. States may, therefore, choose to ignore the DGC if they sense that powerful adversaries are shielding hostile nations.

On the other hand, it is worth noting that at times governments decide to vote against their allies. The Obama administrations final parting shot towards Israel President Benjamin Netanyahu, who repeatedly undermined former US President Obama, stunned the world by abstaining during a UN Security Council vote (UN, 2016[b]). As a result, the Security Council ‘reaffirmed ... that Israel’s establishment of settlements in Palestinian territory occupied since 1967, including East Jerusalem, had no legal validity’ (UN, 2016[b]).

Security is thus a double-edged sword, that strikes both the just and the unjust. With no undisputable international regime able to keep nations in check, the vacuum of power is filled by a multitude of states that engage in the Realist conception of self-help (Evans and Newnham, 1998, p.465). Fundamentally, the cover of cyberspace undermines the ability of Liberalism to guarantee that a state will not secretly engage in cyber-surveillance or CNE that undermines international security and established agreements.

Additionally, Liberalism or liberal notions cannot force states to alert the world to existing flaws that they have discovered in the networks of other nations or organisations. In reference to Smith’s hope that states will report vulnerabilities, the scope and size of a nations intelligence apparatus may prove to be too expansive to give up. As an example

of the low possibility that America would relinquish its vast infrastructure and knowledge of flawed security, the USIC's 'Vulnerabilities Equities Policy (process)' (VEP) is based on storing vulnerabilities for potential use in the present or future (The White House (US), 2017, p.1).

The VEP attempts to help decipher and determine when to disclose information or remain silent in that event that the USG becomes aware of system vulnerabilities that are not public (The White House (US), 2017, p.1). There is a recognition in the USG that disclosing such information is in the national interest (The White House (US), 2017, p.1). Simultaneously, to bolster US national security, 'there are legitimate advantages and disadvantages to disclosing vulnerabilities' (The White House (US), 2017, p.1).

In terms of advantages, awareness of a particular vulnerability can be capitalised upon for 'intelligence collection, military operations, and/or counterintelligence' (The White House (US), 2017, p.1). In reverse, leaving certain vulnerabilities un-remedied leaves USG systems and the public vulnerable to surveillance and cyber-attacks (The White House (US), 2017, p.2). Vulnerabilities, irrespective of whether they are created on purpose or naturally inherent in a network, at times, are known by intelligence services and are stockpiled for their choosing to launch an EI campaign.

America's Department of Defence touched upon this point highlighting that '[a]ll nations have vulnerabilities that can be exploited in and through cyberspace, but we can lessen ours dramatically by harnessing the power of our nation's cyber enterprise' (2015, p.4). As a consequence of knowing that all nations have vulnerabilities, the VEP depicted an opportunistic scenario that the USG has found themselves in, highlighting that:

*At times, intelligence and evidence discovered through judicious exploitation of a vulnerability are the only means to understand a much bigger threat. Often taking a considered risk to restrict knowledge of a vulnerability is the only way to discover significant intrusions that are compromising security and privacy (The White House (US), 2017, p.2).*

However, what happens when that risk backfires and causes havoc all over the world? This was a reality for many countries who suffered significant financial losses at the behest of malicious actors that initiated the WannaCry Hack. During 2018, the US

formally charged PARK JIN HYOK a North Korean programmer for participating in a string of cyber-attacks including the 2017 Wannacry attack, the 2016 Bangladesh Central Bank cyber-heist and the 2014 Sony attack. The above cyber heists appear to be motivated by financial gains and politics rather than propaganda (Cimpanu, 2018; ‘United States Of America v. PARK JIN HYOK’, 2018, p.5-10). Moreover, the ramifications of the WannaCry hack were extensive. According to Smith ‘the nation state-sponsored WannaCry ransomware attack impacted more than 200,000 computers in more than 150 countries and showed the world the broad damage “invisible” cyber weapons can inflict’ (2017[c]).

As the world pondered the source of this cyber-attack, it became clear that the tools used were known by the NSA. In fact, a non-state hacktivist group named Shadowbrokers released NSA computer exploits (vulnerabilities) called ‘EternalBlue and a number of other NSA exploits on the [I]nternet in April 2017. Less than a month later, WannaCry was born’ (Jones, 2017). This gamble left America’s greatest ally in Europe, Great Britain, in a very precarious situation in both the cyber and the physical world. For example, according to a National Audit Office (UK) ‘[t]housands of appointments and operations were cancelled and in five areas patients had to travel further to accident and emergency departments...NHS England identified 6,912 appointments had been cancelled’ (2018, p.10). If large numbers of people had died, how beneficial would the NSA’s code of silence have of been for one of its greatest allies?

Intelligence is supposed to prevent death, not indirectly incite it. Such destruction justifies the need for states to work with each other through a body such as the UN to prevent large scale cyber-attacks from happening. Without a doubt, there is a great need for Liberalism to take its place as a dominant theory through the establishment of a DGC. However, it is unlikely that the US will relinquish its arsenal of vulnerabilities, particularly in the Trump first era. Until a DGC materialises and is binding with significant palpable results; cyberspace will remain in a state of anarchy. As a consequence of this ominous assessment, countries will defend themselves and gather information in the cyber arena to help better protect themselves from domestic threats and international adversaries.

---

### 3.19 Subverting Non-State Efforts

---

Non-state organizations participate within the international arena to assist victims of warfare (War Child 2018; Save the Children, n.d.; The White Helmets, n.d.) and to help states with noteworthy endeavours such as preserving the environment (African Wildlife Foundation, n.d.; Arab Forum for Environment and Development, 2018; Asian Environmental Society, 2018; Climate Network Africa, 2018). Conversely, at times non-state groups find themselves being undermined by powerful states. Despite the noble merits that are tied to the DGC and its underlying liberal institutionalist cosmopolitan roots, the application of this model is riddled with issues that are linked to the behaviour of powerful states. This is not to imply that the model is overwhelming defunct. Instead, it is a negative outlook due to the conditions that such a model has to operate within. These conditions are further polluted with mistrust by powerful states that often choose to violate the rules-based international system in the name of national security.

Indeed, pluralists may perceive international organisations as the ‘harbingers and custodians of a potential community of humankind’, Realist’s may come to view them as ‘instruments of their members, generally of their leading members, which in the case of the UN today would be the US’ (Stern, 2000, p.154). Martin Shaw has emphasised a similar viewpoint in stating that global order is dependent on the choices and desires of powerful Western nations (2005, p.73-74).

I argue that it is not chimerical or outlandish to state that cyberspace will suffer similar setbacks of instability at the behest of powerful states, in spite of non-state institutional efforts. As a means of justifying such a bold assumption, it is vital to analyse the alleged role that the US played in concocting secret plans to subvert the ISO and global encryption standards (Zetter, 2013). The NSA absconded cooperative international measures and sought to use the ISO to undermine global cybersecurity by manipulating members of the ISO into adopting flawed encryption that the US knew how to penetrate. Unsurprisingly, at times international institutions fail at their task of creating global peace because powerful states ‘use their bargaining power as well as their power to structure the choices for others in the construction of institutions’ (Stein, 2010, p. 210). Consequently, powerful states benefit more from the current international order.

The ISO is an international organisation comprised of cryptography and cybersecurity experts from numerous countries, which set encryption standards to secure communications. In the past, the NSA and its representatives to the ISO pushed for its cryptographic standard, Elliptic Curve to be chosen (Menn, 2017). This was eventually accepted and set by the ISO. However, after the Snowden leaks, it became clear that the NSA had ulterior motives with regards to suggesting encryption standards. According to a leaked Snowden document the NSA embarked on inserting:

*[V]ulnerabilities into commercial encryption systems, IT systems, networks, and endpoint communications devices used by targets...Exploit foreign trusted computing platforms and technologies... Make specific and aggressive investments to facilitate the development of a robust exploitation capability against Next-Generation Wireless (NGW) communications (EFF, 2013[a], p.1).*

The damning part of this revelation was the fact that the US sought to steer the ISO to get encryption standards favourable to them. In other words, America wanted to set a standard that the USIC knew how to subvert. According to an excerpt from the Snowden leaks, US intelligence aimed to influence policies and specification for commercial, public key technologies to ‘[s]hape the worldwide commercial cryptography marketplace to make it more tractable to advanced cryptanalytic capabilities being developed by NSA/CSS’ (EFF, 2013[a], p.1-2).

In light of this shameful revelation, it is clear to observe that even when presented with the opportunity to comply with independent institutions, the US schemed to undermine it. Why some observers might ask? Simply because America has the vast capacity to do so. So long as the technology exists, and perceived threats to US dominance and national security exist, cyber instability will not cease. Previous endeavours by the former US Secretary of Defence Donald Rumsfeld to “Fight the Net” as a means of dominating the information spectrum have clearly not changed since 2003 (Rumsfeld, 2003, cited in National Security Archive (US), 2006[b], p.10).

As a consequence, this leaves people distrustful of the USG and concerned about cybersecurity. Of recent, the NSA’s encryption algorithms SIMON and SPECK were rejected by the ISO (Schneier on Security, 2018). Israeli delegate Orr Dunkelman

highlighted concerns stating that '[t]here are quite a lot of people in NSA who think their job is to subvert standards. My job is to secure standards' (Menn, 2017). Such concerns hamper the ability of NGO's and IGO's to work effectively and deliver safe products to those whom they serve. Theoretically, Liberalism can work in an ideal setting. Ultimately cyberspace remains anarchic and subject to propaganda and surveillance measures.

To conclude, at this stage, I have covered and juxtaposed both Liberal and Realist theories, EI, stockpiling vulnerabilities and the consequences of doing so. Liberalism as a theory is needed in cyberspace to protect civilians and organisations. As it stands, cyberspace is an incredibly anarchic domain to which propaganda and intrusive surveillance flourish. Moving forward, one day, a cataclysmic event concerning cybersecurity may force states to abandon Realist fears and embrace a liberal approach to IR and cyberspace norms. Until then, the world will continue to witness events in which countries, organisations and citizens are victims of intrusive surveillance. As such, Realism is not dead or obsolete. Realism has been reborn in cyberspace flanked by propaganda and surveillance, two tools that are used to reap havoc.

---

## Chapter 4: Literature Review

### 4.1 The Surveillance Literature Review

---

The act or process of surveillance stretches back thousands of years. Antiquated religious books such as the bible are filled with cases of surveillance. Before Jesus was executed, his enemies had sent spies to provoke him into saying something outlandish to have him arrested (Luke 20:19-25). Since the Bible, scholars such as Lyon have described surveillance as 'a central feature of modernity' (1994, p.37). For the sake of clarity 'surveillance involves the purposive monitoring of conduct to allow for the identification, acquisition and classification of information with the intention of modifying that conduct in some manner' (Innes, 2003, p.113). The latter part of this definition 'modifying conduct', in a post-Snowden era reflexively highlights the power aspect of those who are in positions to contort and hold large swathes of information. On the other hand, benign surveillance measures such as managing outbreaks of diseases that are predicated on a

‘quarantine’ of humans or health databases that track outbreaks of diseases are unlikely to be seen as Orwellian (O’Hara and Shadbolt, 2008, p.31).

Similarly, in the view of Clive Norris and Gary Armstrong ‘[t]he modern state would be inconceivable without such systems. How else would taxes be collected, entitlement to welfare benefits be adjudicated, the spread of infectious diseases controlled, law enforced and punishment delivered?’ (1999, p.5). Indeed, the process of surveillance encompasses some benefits to humankind. However, issues begin to surface when surveillance is focused in certain areas or at specific people. Those that admired Princess Diana may deem it inappropriate that the NSA allegedly held ‘1056 pages of fairly recent transcripts relating to Princess Diana’ (Parker, 2000, p.117). Also, greater social ills such as social biases can become problematic for surveillance assemblages and society as a whole. According to Tina Patel:

*[S]urveillance selectively over-focuses on those it perceives or seeks to label as deviant, which, within a white majority society gripped by terror-panics, refers to all those of middle Eastern appearance, or of South Asian or Arabic heritage and of the Muslim faith, or, what I have termed ‘brown bodies’ (Patel, 2012, p.230).*

This is an experience that African American activists have endured since the height of the civil rights period (the 1960’s) to contemporary Black Lives Matter activists that have been tracked by the FBI (National Archives and Records Administration (US), 2016; Joseph and Hussain, 2018). Aside from race, people from multiple professions and backgrounds have been targeted by surveillance. In the UK, Special Branch Intelligence officers ‘passed information to a controversial network that blacklisted construction workers’ (Casciani, 2018). Similarly, researchers at Citizens Lab were right to point out that Russian based hacker’s targeted civil society to monitor and exfiltrate sensitive information (Hulcoop et al., 2017).

For decades Michele Foucault’s interpretation of Jeremy Bentham’s Panopticon has held sway over the extent to which surveillance has perceivably had an impact on modern society in terms of visibility, power and control. Jonah Bossewitch and Aram Sinnreich have described the Panopticon as a prison facility that is structured in such a way that ‘inmates know they are being watched, though they do not always know when’ (2013,



p.230). The inmate is ‘seen, but he does not see; he is the object of information’ (Foucault, 1991, p.200). Within the Panopticon, the inmate can see parts of the central tower in which the guard is present but ‘must never know whether he is being looked at at any one moment’ (Foucault, 1991, p.201). It is this unequal relationship between the guard and the inmate that produces Panoptic power, and the element of risk that exacerbates the inmate’s anxiety and fear of being observed (Foucault, 1991, p.202). Consequently, this consistent heightened awareness gives rise to a ‘fictitious’ atmosphere in which the inmate becomes ‘the principle of his own subjection’ (Foucault, 1991, p.202-203).

In short, the Panopticon aims to produce self-discipline as opposed to previous draconian tactics of coercion in human history, such as torture (Lyon, 2006, p.3). As such, society to some degree can be viewed as a Panopticon due to the pressure that surveillance places on citizens to submit to state norms. Moreover, Jean-Paul Sartre’s Phenomenological Ontology of *The Look*, emphasises how being monitored is a fundamental phenomenon that alters human behaviour (2003, p.276). Within Sartre’s short tale, a nosy listener glues his ear to the door in an attempt to eavesdrop on an unwitting individual on the other side.

Immersed in his activity, the eavesdropper’s ‘consciousness sticks’ to his acts (of listening) and thus becomes ‘drunk in by things’ (Sartre, 2003, p.283). In other words, his ‘reflective consciousness’ concerning his dishonourable act has significantly become reduced (Sartre, 2003, p.284). However, suddenly, a passer-by catches the eavesdropper in the act. At this particular juncture, the look of the individual, causes the eaves dropper’s consciousness to become detached from his previous actions and experiences discomfort. In many respects, being monitored by another consciousness has a profound impact on how humans perceive themselves and has the potential to influence human behaviour.

On the other hand, in the 21<sup>st</sup> Century, the Snowden affair has emphasised how easy it is for nations to keep track of foreign governments and vast swathes of citizens. The far reach of modern surveillance structures has meant that all categories of people fall under the observation of multiple surveillance assemblages within various levels of society. In many respects, ‘[s]urveillance is not directed exclusively at the poor and dispossessed, but is now omnipresent, with people from all segments of the social hierarchy coming under scrutiny’ (Haggerty, 2006[b], p.29). This includes those in power such as police officers that within the Bentham paradigm of the Panopticon, that invoke the gaze.

Technological advancements have provided the world with video recording smartphones which allow protestors to reverse surveillance, thus bringing Foucault and Bentham's conception of the Panopticon into disrepute. Influential observers become observed, allowing those who are so used to being the target of surveillance to fight back and exercise a form of power.

The shift in power has been referred to as *sousveillance* which has played a pivotal role in capturing police brutality towards unarmed African Americans such as Eric Garner, and George Floyd (Mann and Ferenbok, 2013, p.19; The Guardian, 2014). *Sousveillance* focuses on enhancing the ability of people to access and collect data about their surveillance and to neutralise surveillance (Mann, Nolan and Wellman, 2003, p.333). From this angle, the traditional view of surveillance as being 'like 'God's eye in the sky'' has shifted (Lyon, 2014[a], p.30). This is not to imply that the effects of Panopticism has been extirpated by advanced electronic surveillance, but simply altered.

Furthermore, it is vital to note that control obtained through surveillance is not indefinite. According to Lyon, '[t]he most panoptic circumstances do not necessarily produce the most docile bodies' (2006, p.6). This was most certainly the case when Julian Assange, the founder of WikiLeaks, continued to comment on matters concerning surveillance despite previously being huddled up in the Ecuadorian embassy with British police outside waiting for him to leave. On the flip side, in some cases *sousveillance* does not have a significant amount of control over those being watched, considering that in the US, police officers continue to engage in modern day lynchings of unarmed African American men amidst multiple body-cams and smartphones being present (The Guardian, 2014). Having acknowledged Lyon's perception of surveillance, it is crucial not to create a deductive association between surveillance and ultimate control. In support of this view, Norris and Armstrong suggested that '[w]e need to be cautious about merely equating the power to watch with the disciplinary power implied in Foucault's concept of panoptic surveillance' (1999, p.6).

Additionally, some citizens in the Panopticon have grown to like being observed to the extent that it has become a liberating factor for society. For example, Facebook provides millions of users around the world an opportunity to gaze at other people's personal information without the need of being acquainted in the physical world. Conversely, it is

important to note that behind this liberating aspect is the hand of intelligence services that are culling data for surveillance purposes, thus re-appropriating an element of power. More so, an NSA analyst pointed to an emphatic irony concerning digital information and the gaze: ‘Who knew in 1984 that this [Apple iPhone] would be Big Brother...and the zombies would be paying customers?’ (EFF, 2013[b], p.1-3).

On the other hand, since the above quote was revealed, Facebook users still seem happy to live with multiple observers. This reality serves as a reminder that portions of society crave attention and visibility. With so much on show, without companies having to fight tooth and nail to gain access, Orwell may have struggled to adjust to the modern cyber era.

---

## 4.2 Post Snowden

---

While it would be near impossible to gather and juxtapose literature concerning every single NSA, GCHQ or Five Eyes program exposed by Snowden, it is vital to review modern surveillance practices by intelligence services in conjunction with academic assessments. To begin with, in the view of David Fidler GCHQ intelligence programs such as Tempora, gathered ‘large volumes of metadata and communication content by accessing fibre-optic cables’ (2015, p.200). The NSA’s Prism program collects information from servers of US service providers (Greenwald, 2014[b], p.108). Furthermore, the NSA’s Upstream program ‘captures data by tapping directly into fiber optic cables, digital hubs, and routers’, whereas Boundless Informant ‘captures global metadata on communications of all kinds’, have become a cause for concern (Masco, 2017, p.397).

Despite the UK governments claim that its surveillance practices are not tantamount to mass surveillance, Lyon’s assessment underscores the scale of British activity in stating that, ‘American, British, Canadian, and possibly other agencies – engage in astonishingly large scale monitoring of populations’ (Lyon, 2014[b], p.2). Fundamentally, the Tempora program appeared to be a ‘dragnet’ which caused outrage in the British media once Tempora was exposed (Lyon, 2014[b], p.2). Unsurprisingly, former GCHQ director Sir David Omand has taken quite the opposite stance to Lyon in suggesting that:

*[T]he media fall into the category error that has crept into much of the recent public debate of not distinguishing bulk access by computers to the [I]nternet – which the US and UK certainly do have – and so called ‘mass surveillance’, which they do not conduct. Mass surveillance implies observers, human beings who are monitoring the population. As the UK Interception Commissioner confirms, no such mass surveillance...takes place by GCHQ (Johnson et al., 2014, p.806).*

Furthermore, Omand went to the extent of stating that there is no secrecy scandal concerning the Snowden leaks and GCHQ (Johnson et al., 2014, p.805). While it is true that media stories about intelligence can capture the imagination of the public due to the exciting way this field is portrayed in the film industry, dismissing the significance of the Snowden leaks is a questionable move. Researchers such as Alrich and Moran have chosen to describe the Snowden revelations as ‘mass surveillance programs’ which would appear to contradict Omand’s nonchalant perception to this issue (Johnson et al., 2014, p.795). In hindsight, the existence of GCHQ and NSA programs raises the question of risk in modern society.

As a consequence of Snowden’s controversial leaks, ‘[w]e have become aware of the potential catastrophe only because a single private contractor working for the CIA applied the means of information control in order to tell the world about the global digital risk’ (Beck, 2016, p.142). Risk and the digital world have thus become entangled further due to action taken by Snowden. Moreover, in response to the Snowden affair, Beck has asserted that:

*The PRISM scandal has opened up a new chapter in world risk society. In the past decades we have encountered a series of global public risks, including the risks posed by climate change, nuclear energy, finances and terrorism – and now we face the global digital freedom risk (Beck, 2016, p.141).*

Accordingly, Beck went on to criticise and explore the future of democracy, which appeared to be rather bleak, as a side effect of mass surveillance:

*The Snowden revelations regarding mass surveillance exemplify another ‘emancipatory catastrophe’. On the one hand, they are triggering an anthropological shock by revealing that, and how, democracies are becoming*

*metamorphosed insidiously and imperceptibly into totalitarian regimes. This process of the metamorphosis of democracy can produce a new form of totalitarian control behind the façade of functioning democracy and the rule of law (Beck, 2016, p.146).*

From Beck's perspective, surveillance and control that have been afforded to governments have made this practice an irritant to democracy, thus posing questions to surveillances viability in the long-term. In the past, Lyon suggested that '[f]or many people, connecting computer power with surveillance in the realm of the state is a sure way to activate the hairs on the back of the neck!' (1994, p.86). It would thus appear that Beck's more recent ominous picture of the situation at hand qualifies Lyon's past suggestion that surveillance is something to be concerned about. However, it is essential to recognise that the degree of risk which citizens are exposed to has the potential to be challenged, as a result of public awareness of the previously mentioned surveillance programs. Following this view, Maria Murphy juxtaposes both past and present reactions to surveillance scandals:

*Just as there had been calls for investigation and open evaluation following the Watergate leaks, there were calls for reform in the wake of the Snowden revelations. By shining light on the covert practices of the NSA, Snowden empowered the public to express whether or not they were satisfied with the – previously secret – status quo (Murphy, 2017, p.205).*

Therefore, in accordance with this democratic principle '[w]ithout doubt, Snowden is right to raise issues of privacy, civil liberties—including freedom of expression, communication and assembly—and human rights in relation to what his findings have exposed about the NSA and its cognate agencies around the world' (Lyon, 2015, p.143). Although Snowden's actions are illegal, the evidence cited above is indicative of the fact that his actions have changed the course of the debate surrounding what is unacceptable from democratic governments in relation to surveillance.

---

## 4.3 Privacy and surveillance

---

Knowledge of large scale surveillance operations can cause domestic and international concerns about privacy. According to O'Hara and Shadbolt, 'there are many tangible benefits to be gained by allowing intrusions into one's life, but there is also the intangible worry' (2008, p.5). The possibility that influential people with advanced monitoring equipment can monitor millions of people is a daunting thought, particularly considering that Western nations have excelled in the field of surveillance. Additionally, O'Hara and Shadbolt have suggested that '[t]he usual understanding of privacy is to do with a subject's control of information about him or herself' (2008, p.18). Similarly, Andrew McStay advocates a near-identical view and has suggested that '[p]rivacy in a liberal context is predicated on the capacity to manage access to one's life' (2014, p.24).

McStay's understanding spells out the issue with privacy in the modern era, as the Snowden revelations have shown that vast amounts of data about citizens all over the world are in the databases of the NSA and GCHQ. When citizens look for a guardian to ensure that their privacy is protected, the issue of privacy becomes further inflamed. Beck summarised the gloomy outlook for citizens in conjunction with the idea that governments cannot be trusted to protect citizens from privacy risks:

*After all, which powerful actor is interested in ensuring that people continue to be aware of this risk, thus pushing the public towards political action? The first actor that comes to mind is the democratic state. But, alas, this would be like asking the fox to look after the chickens. Because it is the state itself, in collaboration with the digital entrepreneurs, that has established the hegemony over data in order to optimize its key interest in national and international security. The extensive enmeshment of private and public resources of control in this field means that we are moving in the direction not of a 'world state', as many anticipated, but of an anonymous digital central power that controls the private behind a democratic façade (Beck, 2016, p.144).*

While many governments would be insulted by the words of Beck, the vast amount of literature cited thus far indicates that governments are the perpetrators of massive privacy invasions. Therefore, it is a tragic irony that citizens need to turn to what many would see

as the source of the problem. McStay offered a similar outlook which again, emphasises the ironic risk of trusting liberal democratic governments: ‘[t]he problem for liberals is that governments cannot be relied upon to safely look after such information in a responsible and open fashion so to be properly accountable to the people it governs’ (2014, p.23-24). With such a bleak picture in mind, it begs the question of what citizens should do to protect themselves. Is it logical or appropriate for citizens to abandon digital technology to protect their privacy?

---

## 4.4 Ontological Security

---

Of late, IR academics have incorporated the sociological term OIS within the field of IR. In particular, the concept of OIS has been used in relation to the EU’s sense of self amidst EU sceptics (Johansson-Nogués, 2018, p.532), New Zealand’s trade with China, (Young, 2017, p.513-514), Britain’s ‘imperial ontological (in) security’ concerning Afghan rulers during Anglo-Russian competition in Central Asia (Bayly, 2015, p.817-818) and the perception of German anxiety over international pressure to lead in Europe (Karp, 2018, p.58). Despite the sizable amount of interest that OS has received from IR scholars, some have strong reservations for adopting the concept into the lexicon of IR.

According to Stuart Croft and Nick Vaughan-Williams ‘should such studies be developed at all, or should they be kept in a position ‘outside’ the legitimate space of IR, confined to other parts of the social sciences, to keep the discipline more focused?’ (2016, p.13). Ayşe Zarakol also raised this focal talking point by articulating the concern that ‘[s]ome have objected to the transfer of the concept into IR by countering that states do not have ‘selves’ and therefore cannot ‘care’ about ontological security’ (2016, p.48). Conversely, in a poignant self-rebuttal, Zarakol alluded to the point that:

*If states do not have selves, they also cannot ‘care’ about their physical survival or be thought of as purposeful rational agents. Without ontological security, the self cannot know where it begins and ends, and what is essential to the body (and its survival) can only be defined by the self (Zarakol, 2016, p.48).*

In the real world, it is clear that states do care about how they are perceived. National anthems often contain truncated elements of self-prescribed national tropes. Furthermore, governments and citizens often take a great amount of pride in national flags even though they are inanimate objects. Moreover, the debate over whether OS is worthy of being adopted into the lexicon of IR can be settled by looking at previous scholarship concerning territorial conquest and ‘state denial of historical crimes’ (Zarakol, 2010, p.3).

To begin with, OS ‘proposes that states seek not just physical security, but security of the self (ontological security) in the form of their own identity, and, as such, seek to define themselves in terms of both their actions and those of other states, and their respective identities’ (Bayly, 2015, p.820). States often seek to construct stories that justify their existence and the righteousness of actions that make the nation appear noble. Louis Pérez’s in-depth research into US opinion over Cuban independence serves as a reservoir of ideological thought for which one can draw insight into how America constructed its OS in relation to Cuba. According to Pérez:

*To enter the logic of the geostrategic calculus of the 19th century is too readily understand how the Americans persuaded themselves of the need to possess Cuba. Lying astride the principal sea-lanes of the middle latitudes of the Western Hemisphere, on one side commanding the entrance to the Gulf of Mexico and the outlet of the Mississippi Valley and on the other fronting the Caribbean Sea, the island assumed commercial and strategic significance of looming proportions. It became all but impossible for the Americans to contemplate their future well-being without the presumption of possession of Cuba (Pérez, 2008, p.25).*

Persuasion concerning the desire to acquire Cuba came from prominent figures such as John Quincy Adams who referred to Cuba as the ‘object of transcendent importance to the political and commercial interests of the union...The annexation of Cuba to our Federal Republic will be indispensable to the continuance and integrity of the union itself’ (US Congress, House of Representatives, 1852, cited in Pérez, 2008, p.25). In spite of the critique levelled by Croft and Vaughan-Williams, both examples above indicate that the American self, irrespective of where it is located, perceived a great sense of danger to its physical self and its ideological or ontological self. The destruction of the US Union



would thus bring about an end or at least greatly curtail America's ontology. Therefore, it is clear that the state can have a sense of self.

Moreover, this topic can be further dissected by looking into Japan's alleged educational textbook revisionism. Japanese textbooks were condensed fragments of official ontological and historical reasoning, which helped to steer the narrative or lack of narrative on issues such as military aggression towards its neighbours and South Korean comfort women. According to Yoshiko Nozaki, in the case of Japan's 1981–82 textbook screening, Tokyo was accused of misconstruing 'Japanese wartime atrocities in Asian countries and Okinawa' (2002, p.606). This led to international protests, particularly from South Korea and China (Nozaki, 2002, p.606).

Concerned about its image and standing with neighbours such as South Korea, Japan apologised for its use of 'comfort women' or forced prostitution of Korean women during WW2 to alleviate its sense of OIS and strained relations with South Korea. In 2015 the Japanese Prime Minister Shinzo Abe acknowledged this issue by stating that "Japan and South Korea are now entering a new era... We should not drag this problem into the next generation" (Abe, 2015, cited in Calamur, 2015). This can be viewed as an attempt by Japan to alter its image and construe a new ontological identity that is not predicated on historical crimes. Judging from the above literature, Japan's neighbours were disgruntled because their identity as a victim that eventually triumphed over an aggressor is being undermined. It is this sense of self or identity that enables states to assume roles or stances during relations with others.

In addition, from Karl Gustafsson's perspective on OS and history, in order to maintain an ontological self, nations such as China have taken alternative approaches to 'immunise Chinese citizens against such threats' concerning Japanese history. This has taken the form of war museums that are referred to by the Chinese government as 'patriotic education bases' (Gustafsson, 2014, p.73). Moreover, amidst the social cartoon crisis that took place in Denmark (in 2005-2006), Sweden (in 2007) and the Charlie Hebdo attack in France (in 2015), individual as well as State OS was egregiously on display (Jorgensen, 2006; Larsson and Lindekilde, 2009, p.361-362; Dawes, 2015, p.1). Offensive cartoons that targeted Islam and the Prophet Muhammed incited a backlash from Muslim communities in Denmark and Sweden. As stated by Christine Agius:

*[C]artoon crises represent a complex discursive performance of identity that speaks to a broader set of ontological security concerns which intersect at the international, regional and national levels...Swedish and Danish discourses show the tensions associated with the desire for a stable and consistent idea of self when contrasted with the Muslim 'other' (Agius, 2016, p.109).*

In the case of France, the Charlie Hebdo terrorist attack in many respects, reinforced how France perceived itself as a liberal state that tolerates free speech, including offensive satire (Bamat, 2015). In this context, states have selves which manifest as recognisable nationwide tropes, e.g. France is a liberal state. While it is challenging to locate an exact location for the self, to dismiss this notion would be to dismiss the idea that an individual does not have selves or contrasting personality traits on the premise that it is challenging to locate the self in the mind or inside the brain of an individual.

---

## 4.5 Hacktivism

---

In the digitised 21<sup>st</sup> century where secret documents and leaks concerning election scandals, propaganda campaigns, surveillance activities, intelligence services and tax havens are revealed to the world (by leaks), citizens have become far more exposed to the behaviour of elites and governments than ever before in history (Greenwald, 2014[c]; WikiLeaks, 2017[a], p.108; WikiLeaks, 2017[b]; European Parliament, 2017, p.21). Some enjoy the phenomenon of hacktivism as it purports to bolster transparency and align people with a more inclusive form of democracy, as opposed to allowing intelligence services to hoard important information. Andrew Schrock presents a slightly positive depiction of hacktivism concerning democracy and civic participation:

*The civic hacker tends to be described as anachronistic, an ineffective "white hat" compared to more overtly activist cousins. By contrast, I argue that civic hackers' politics emerged from a distinct historical milieu and include potentially powerful modes of political participation. The progressive roots of civic data hacking can be found in early 20th-century notions of "publicity" and the right to information movement (Schrock, 2016, p.581).*

Hacktivists such as WikiLeaks have helped to enlighten millions of people around the world about the dark dealings of governments, which in turn has allowed the public to have a more meaningful stake in politics. In the view of *The Economist*:

*If secrecy is necessary for national security and effective diplomacy, it is also inevitable that the prerogative of secrecy will be used to hide the misdeeds of the permanent state and its privileged agents. Organisations such as WikiLeaks, which are philosophically opposed to state secrecy and which operate as much as is possible outside the global nation-state system, may be the best we can hope for in the way of promoting the climate of transparency and accountability necessary for authentically liberal democracy* (*The Economist*, 2010).

Reflexively, it is difficult not to contemplate the ‘apparent clash between the ideal of a deliberative democracy to provide the public with information about actions at the political level’ amidst organisations such as WikiLeaks that break the law to deliver secret information in the name of democracy (Ronn, 2016, p.765). As a consequence, the equilibrium between the public and the state has shifted at the expense of leaving democracy in a paradoxical state of inclusion and risk.

---

## 4.6 Democracy and Intelligence

---

Irrespective of the political system that a nation chooses to adhere to, Angela Gendron has suggested that ‘[i]ntelligence is one means by which a nation-state pursues its obligation to protect the interests and rights of its citizens’ (2005, p.398). Authoritarian regimes and democracies make use of intelligence. In authoritarian regimes, how information is attained is not as controversial as it would be in Western democratic countries. In the assessment of Zakia Shiraz, intelligence services within the global south are preoccupied with protecting regimes from domestic subversion and international strife (2013, p.1755). In other words, governments from the global south tend to use the intelligence apparatus to protect the regime from opposition by internal and external threats. On the other hand, academics such as Marina Caparini have described the role

and limits that intelligence services should have within a democratic state. According to Caparini:

*A fundamental precept of democratic theory is securing and maintaining public consent for the activities of the state... Intelligence agencies must be perceived as performing a necessary function, operating efficiently and effectively, accountable for their actions and those of their members, and under the firm control of elected authorities (Caparini, 2007, p.3).*

Conversely, security and intelligence services operate in an environment that in many cases, is not unequivocally bound to egalitarian ideas due to the need to subvert targets. As noted by Caparini, ‘the intelligence sector is also a special area of state activity. It has a vital role in safeguarding national security (and in some extreme cases, the survival of the state), resulting in a strong imperative for secrecy’ (2007, p.3). The special designation of breathing space that intelligence services are provided can induce limitations of oversight which lead to gross abuses and scandals.

A perfect example of this point was South Korea’s intelligence services that attempted to influence the 2012 presidential election (BBC, 2017[b]). Avoiding scandals witnessed in South Korea’s presidential elections requires the government to directly or indirectly control and monitor surveillance by an elected regulatory body. Although the distance between a nation’s Parliament and intelligence services is necessary to avoid the possibility of intelligence that cajoles or pleases politicians.

Although controversial, the National Security Archive has alleged that the NSA skewed evidence in favour of strikes on Vietnam during the infamous Gulf of Tonkin incident. According to National Security Archive Research Fellow John Prados, ‘[t]he parallels between the faulty intelligence on Tonkin Gulf and the manipulated intelligence used to justify the Iraq War make it all the more worthwhile to re-examine the events of August 1964 in light of new evidence’ (National Security Archive (US), 2005). Similarly, NSA historian Robert Hanyok has suggested that the ‘incidents, principally the second one of 4 August, led to the approval of the of the Gulf of Tonkin Resolution by the U.S. Congress, which handed President Johnson the carte blanche charter he had wanted for future intervention in Southeast Asia’ (2005, p.2). If this allegation is true, democracies

should be concerned that intelligence can be skewed for politicians and military figures. Although it is important to note that this account is a highly contentious and an unresolved debate (Giles, 2005, p.3).

While it is clear is that intelligence services require leniency and space to engage in covert operations, while simultaneously requiring some form of connection to regulatory organisations in order to prevent skewed intelligence from impacting government policies. As a means of avoiding foul play by rogue intelligence officers, John Hollister Hedley has indicated that a regimented objective standard should be prescribed for intelligence services to embrace.

From Hedley's perspective, it can be claimed that '[i]ntelligence professionals must learn to check their political views and policy preferences at the door, and not allow them to colour the rendering of professional judgment at any step of the intelligence process' (A Symposium on Intelligence Ethics, 2009, p.368). In the UK, intelligence operatives and analysts must be politically objective. According to MI5, intelligence services within a democracy need to be apolitical (n.d.[e]). Political objectivity is crucial as a means of avoiding democratic issues such as election meddling.

On the other hand, weaker democratic institutions in other parts of the world may not concur with the MI5's view on the standards that analyst and operatives should embrace. Florina Matei and Thomas Bruneau have written emphatically concerning new democracies with little experience of transparency and restraining intelligence services (2011, p.657). With regards to new democracies that were previously authoritarian, intelligence services are at risk of simply returning:

*[A]s political police (with the politicians using them to deter and remove potential political adversaries, control aggressive investigative journalists, and deflect other possible opponents), or as independent security states, functioning for their own purposes' (Matei and Bruneau, 2011, p.663).*

This may be due to intelligence operatives and their superiors still clinging on to the ways of the past, albeit with a democratic shell to appease citizens and international critics. Literature concerning Brazil's democratic reform of intelligence agencies highlights the fears cited by Matei and Bruneau. According to Joannisval Gonçalves '[d]uring the works

of the Committee, the Parliamentarians discovered more than 375,000 irregular interceptions to support police investigations in 2007. The main diagnosis of the security and intelligence system was that it was completely out of control' (2014, p.595). Considering Brazil's human rights abuses inflicted by its intelligence services under military dictatorship, Gonçalves's assessment is an example of young democracies failing to let go of dangerous habits.

This was a prominent case in South Africa back in 2012 when its intelligence service used a spy with access to the Russian government to ascertain information concerning 'its own government's involvement in a \$100m (£65m) joint satellite surveillance programme with Russia... known as project condor' (Milne and MacAskill, 2015). Judging from figure 23, one can observe the dangers of partisan desires that eventually traverse a dangerous Rubicon. In the long term, such activity may push factions within a government to rely on their contacts as opposed to approval by an independent Parliamentary committee.

TOP SECRET	
<b>QUALITY ASSURANCE</b>	Has the product been through the Chief Directorate Clearance Panel?
	Has the Deputy-Director's Clearance Panel recommended this product?
<b>THE EVENT</b>	: RUSSIAN INTELLIGENCE – STRATEGIC COOPERATION WITH SOUTH AFRICA : 21 AUGUST 2012
<b>ACCURACY STATEMENT</b>	: (To be determined by EXCO)
1.	Agent <b>AFRICANIST</b> with direct access to the Russia Government provided the following s update regarding Russian Intelligence (SVR) and Russian military Intelligence (GRU) interaction with South Africa.
2.	Agent provided a short overview regarding the status of continued cooperation between South Africa (DENEL / SANDF) regarding the aerial satellite surveillance programme Project <b>CONDOR</b> . Russian GRU member [REDACTED] (formerly posted to South Africa in a declared capacity) and former Head of the SANDF's Military Intelligence General <b>MTAU</b> (believed to be with DENEL) remain key role players in respect of <b>CONDOR</b> .
2.1	Project <b>CONDOR</b> is regarded as a significant part of the envisaged strategic cooperation between the two countries that would culminate in the launch of a satellite by Russia on behalf of South Africa, hopefully by 2013, placing South Africa in a position to conduct its own aerial surveillance in Africa, potentially right up to Israel for strategic military purposes. Currently there are 30 Russian technicians working in South Africa in close cooperation with South African authorities on the project.

Figure 23: Al Jazeera, 2015, cited in Jordan, 2015, p.2

---

## 4.7 Ethics of Intelligence and the Democratic State

---

In an ideal democracy, operatives would be able to gather intelligence without infringing upon any ethical codes. Far removed from this moral utopia ‘[i]ntelligence-gathering has never been a straightforward business in terms of the ethical issues it raises for a liberal society’ (Richards, 2012, p.761). Before addressing the issue of intelligence, it is important to unpack and describe the word, ethics, and the concept of truth-telling. As described by Michael Herman ethics combines ‘ideas of personal morality and social utility; on the one hand, the dictates of good conscience, and on the other accepted standards (or ideals) of human intercourse and the social consequences if they are flouted’ (2004, p.343).

Also, according to Stuart Farson ‘[t]ruth telling is deeply embedded in many of the world’s cultures and religions. It is an intrinsic dimension of democratic governance. . . Truth telling is also an essential component of the criminal court system’ (A Symposium on Intelligence Ethics, 2009, p.382). With such a high bar being set, one has to ponder whether ethics and intelligence gathering can coincide smoothly. In direct contrast, Farson has indicated that ‘lying and deception are often said to be essential features of intelligence work, even in democratic states’ (A Symposium on Intelligence Ethics, 2009, p.382).

Furthermore, Loch Johnson has described intelligence as consisting of ‘stealing secret documents from adversaries; bribing disreputable individuals to spy against their own countries; planting propaganda in newspapers and magazines overseas; and plotting to overthrow foreign governments’ (A Symposium on Intelligence Ethics, 2009, p.367). Considering this assumption, Johnson was right to ask, ‘[w]hat does all this have to do with morality?’ (A Symposium on Intelligence Ethics, 2009, p.367). So far, it is evidently difficult to conflate intelligence and ethics together in harmony. Often the end result of intelligence services engaging in insidious intelligence operations may incite the feeling of being in a surveillance state. However, seldom do intelligence operations secrete regular in depth updates to citizens about sensitive intelligence matters. The feeling that

morality and intelligence are opposed can be a prominent notion. In fact, according to the British Cabinet Office's National Intelligence Machinery report:

*Secret intelligence is information acquired against the wishes and (generally) without the knowledge of the originators or possessors. Sources are kept secret from readers, as are the many different techniques used. Intelligence provides privileged insights not usually available openly (Cabinet Office (UK), 2010, p.38).*

Infringing on the privacy and rights of citizens in a democratic nation does not appear to be a liberal phenomenon. From the off start, the amalgamation of ethics and intelligence seems fraught with strife. However, Michael Quinlan has offered an alternative viewpoint, explicitly stating that '[i]t is not obvious that this is in itself seriously wrong in moral terms; in ordinary life it may often be a breach of courtesy or social convention, but scarcely a grave evil' (2007, p.4). On a similar and lighter tone, Herman has described Intelligence as 'information gathering' in which 'no one gets hurt by it, at least not directly' (2004, p.342). Considering that intelligence operatives work in the shadows gathering data that some people may never know has been collected, Herman's point holds true that no one is physically hurt.

Perhaps so, unless an innocent civilian becomes collateral damage from a drone strike on the other side of the world. While there are elements of truth to Herman's suggestion, in a broader context it is difficult to defend this assertion in light of America's global drone wars and civilian casualties (Lewis and Vavrichek, 2016, p.3). These concerns came to light during the Obama administration when two al-Qaida hostages were accidentally killed in a US drone strike back in 2015. During a public apology, former US President Obama stated that:

*Based on the intelligence that we had obtained at the time, including hundreds of hours of surveillance we believed that this was an Al-Qaida compound, that no civilians were present and that capturing these terrorists was not possible. And we do believe that the operation did take out dangerous members of Al-Qaida. What we did not know, tragically, is that Al-Qaida was hiding the presence of Warren and Giovanni in this same compound. It is a cruel and bitter truth that in*



the fog of war generally and our fight terrorists specifically, mistakes, sometimes deadly mistakes, can occur (Obama, 2015, cited in The Washington Post, 2015).

Needless to say, people can be hurt by intelligence failures even if intentions by the perpetrator were righteous. At this early stage of the debate concerning ethics and intelligence, it would appear that both the former and the latter (ethics and intelligence) produces an 'oxymoron' (Johnson, 2009, p.367; Clarridge, 2006, cited in Shane, 2006).

The oxymoronic aspect of intelligence is based on the equilibrium between operating in a Cold War Realist world of competition, subversion, surveillance, propaganda and warfare while trying to maintain the utopia of living by a higher democratic standard. For example, according to Johnson '[t]he United States is a democracy, with a proud tradition of fair play in international affairs and a desire to be a respected world leader' despite its aggressive intelligence and covert adventures abroad (A Symposium on Intelligence Ethics, 2009, p.367). However, according to former CIA and NSA boss, General Michale Hayden, '[w]e kill people based on metadata' (Johns Hopkins University, 2014).

In direct contrast to Johnson's claim is the blunt reality in which nations violate laws of other countries to gain intelligence and carry out lethal attacks. During the peak of the Snowden leaks, the former Director of National Intelligence, General James Clapper highlighted that 'leadership intentions, in whatever form that's expressed is kind of a basic tenant of what we are to collect and analyse' (CNN, 2013). Such a bold yet honest comment from General Clapper brings to light the difficulty of applying intelligence operations cordially and politely within the international arena.

Intelligence activity is often problematic within the international arena that contains over 190 state actors who are potentially violating the laws of other nations while clinging on to noble ideals of a rules-based international order. At this juncture, it is evident to see why intelligence and ethics are seen as an 'oxymoron' (Johnson, 2009, p.367; Quinlan, 2007, p.1). Typically, state survival and the expansion of influence which is often predicated on good intelligence trumps a purist sense of morality.

Moreover, according to Jeffrey Taliaferro '[s]tates under anarchy face the ever-present threat that other states will use force to harm or conquer them. This compels states to improve their relative power positions' (2001, p.128). While states are potentially bound

by their Realist perceptions concerning other countries, it is possible that governments slip into the habit of focusing purely on survival and intelligence gains as opposed to democratic ideals. The Doolittle Report, written by General James Doolittle at the behest of former US President Dwight Eisenhower, suggested that the CIA's Cold War activities should focus on eliminating security threats irrespective of democratic notions of fair play (Office of the Historian, n.d.[d]). General Doolittle argued that:

*It is now clear that we are facing an implacable enemy [Soviet Union/Communism] whose avowed objective is world domination by whatever means and at whatever cost. There are no rules in such a game. Hitherto acceptable norms of human conduct do not apply. If the United States is to survive long standing American concepts of "fair play" must be reconsidered. We must develop effective espionage and counter espionage services and must learn to subvert, sabotage and destroy our enemies by more clever, more sophisticated and more effective methods than those used against us. It may become necessary that the American people be made acquainted with, understand and support this fundamentally repugnant philosophy* (Office of the Historian, n.d.[d]).

It would appear that amoral surveillance and security practices of the state are paradoxically a fundamental part of a common-sense ideal such as state security. Within this context in which there is an aggressive drive to produce intelligence, Goldman has advocated the notion that some intelligence services experience 'Ethicsphobia' (A Symposium on Intelligence Ethics, 2009, p.373). Ethicsphobia 'is the fear of performing ethical conduct' (A Symposium on Intelligence Ethics, 2009, p.374).

In short, the pressure to secure the state can deter intelligence and security personnel from doing the right thing and producing objective and reliable intelligence. In 2016, revelations from the damning Chilcot report revealed cases of intelligence failures that were predicated on the intense geopolitical pressure to obtain evidence that Saddam Hussein had been developing weapons of mass destruction. Cited within the inquiry, MI6 issued a second report on the 23 September 2002 from a source in Iraq which stated that 'VX, sarin and soman had been produced at Al-Yarmuk' were loaded into several containers which also included glass spheres (Parliament. House of Commons, 2016, p.200 [b]).

Initially, this assessment was described by MI6 as valuable intelligence (Parliament. House of Commons, 2016, p.200 [b]). Chilcot went further and revealed that ‘the source had indicated to SIS that he would be able to provide substantial and critical additional intelligence in the near future’ (Parliament. House of Commons, 2016, p.385 [b]). Conversely, according to Chilcot, some months after MI6’s general feeling of confidence in their source, it was noted by MI6 that ‘[b]y December 2002... doubts had emerged within SIS about the reliability of the sourcing chain’ (Parliament. House of Commons, 2016, p.385 [b]). In fact, as early as:

*October, questions were raised with SIS about the mention of glass containers in the 23 September 2002 report. It was pointed out that: Glass containers were not typically used in chemical munitions; and that a popular movie (The Rock) had inaccurately depicted nerve agents being carried in glass beads or spheres. Iraq had had difficulty in the 1980s obtaining a key precursor chemical for soman [a chemical agent] (Parliament. House of Commons, 2016, p.317 [b]).*

Despite this concern, the British members of Parliament and the public were repeatedly told that weapons of mass destruction existed in Iraq, which subsequently paved the way for an act of aggression (War) towards Iraq that killed tens of thousands of civilians. In fact, in the view of Chilcot:

*SIS did not inform No.10 or others that in mid-February 2003 the source had been revealed to have been lying to SIS over a period of time and that it had concluded by early March that there was no further material and that SIS would seek to make direct contact with the sub-source (Parliament. House of Commons, 2016, p.385 [b]).*

It is egregiously clear from this example that ethicsphobia played some part in the decision making of SIS operatives and their political masters. Although there was a catalogue of errors that pushed the UK into a needless war in Iraq, this particular case of ethicsphobia was a focal issue that reinforces Goldman’s concern about intelligence and ethics. It is thus no surprise that Andregg has taken the view that ‘there are some who certainly think that ethics for spies is the dumbest idea ever’ (A Symposium on Intelligence Ethics, 2009, p.366). In contrast, the exact opposite of ethicsphobia, which I

will refer to as ethics-mania poses an equally dangerous threat to democracy than the former. Ethics-mania is the relentless, insatiable desire of intelligence officials, civil servants and sometimes even presidents themselves to directly or indirectly expose intelligence on the principle that one feels they are engaging in a noble deed.

The Trump administration has faced a barrage of leaks from disgruntled employees. For example, according to the former Attorney General Jeff Sessions, the Trump administration has suffered a ‘staggering number of leaks undermining the ability of our government to protect this country’ (Sessions, 2017). This was certainly the case when the New York Times published an anonymous article in which the author an alleged senior figure in the Trump administration, openly stated that ‘[i] work for the president but like-minded colleagues and I have vowed to thwart parts of his agenda and his worst inclinations’ (2018).

At times people who have access to sensitive information, feel justified in being prone to leaking information for the sake of exposing those deemed to be corrupt. From another glance, throughout the Saudi-Turkey Khashoggi affair, streams of leaks concerning the fate of Saudi Journalist Jamal Khashoggi at the hands of a Saudi hit squad within Saudi Arabia’s Turkish based consulate were directed at the behest of Turkish government officials and pro-government media outlets (Gall, 2018).

However, at times ethics-mania does not always have the intended effect. Accordingly, when French Foreign minister Jean-Yves Le Drian was interviewed about President Erdoğan sharing the recorded moments of Khashoggi’s death to world leaders, Le Drian response was “[i]t means that he has a political game to play in these circumstances” (Le Drian, 2018, cited in France 24, 2018). Ultimately, ethics-mania is equally oxymoronic in the sense that it is still questionable whether such leaks should take place. To a great extent, leaks from within a government are symmetrical to the behaviour or the goals of hackers.

---

## 4.8 International Norms, Ethics and Intelligence

---

At this stage of the debate, it is unclear how intelligence and ethics are to be viewed when discussing how states interact with each other on the international scene. In other words, '[h]ow, then, are global moral standards for intelligence activities (i.e., human rights) feasible, and how ought they be authorised and controlled in terms of international, democratic oversight?' (Ronn, 2016, p.764). This was a dilemma that President Obama grappled with back in 2014 when he refused to apologise to Germany and other foreign leaders about the NSA's foreign surveillance operations. During a White House speech in 2014, President Obama bluntly went on to say:

*Now let me be clear: Our intelligence agencies will continue to gather information about the intentions of governments -- as opposed to ordinary citizens -- around the world, in the same way that the intelligence services of every other nation does. We will not apologize simply because our services may be more effective (Obama White House, 2014).*

In contrast, Obama's perception may someday produce the opposite result intended. Needless to say, the production of the USIC report on Russian interference may have been the period when Obama's words came back to haunt America. In addition, Quinlan has suggested that 'while it might be highly interesting to install listening devices in the offices of high functionaries of friendly countries, the penalties of being found out doing so might well greatly outweigh the advantages of knowing whatever might be learned' (2007, p.4). Moreover, an additional issue that various scholars have discussed concerning ethics, intelligence and other nations revolves around the emphasis that governments give to protecting its own population's privacy while relegating foreign citizens to a lesser standard.

To begin with, Allison Shelton has pointed out that domestic surveillance laws that will most likely infringe upon the laws of other nations is 'paradoxical', given that the sometimes self-assumed role of the [US] as the harbinger of democracy' throughout the international arena (Shelton, 2011, p. 26). Regardless of a nation's size and influence, it would be hard to respect the USG scolding another state about mass surveillance and espionage when its intelligence apparatus is global (see chapter 2 and 3).

Back in 2005 Gendron suggested that ‘[t]he basic principle of international law is the sovereign equality of all nations, yet a state’s targeting and tasking of foreign sources and other secret and deniable collection activities abroad fails to respect the individual and collective privacy rights of others’ (2005, p.399). Years after Gendron made the above assertion, Russia attempted to hack the Organisation for the Prohibition of Chemical Weapons (OPCW). Towards the end of 2018, British and Dutch intelligence accused Russia of sending a team of operatives to hack into the OPCW (NCSC, 2018[c]). Perhaps one reason this is still the case is that:

*Intelligence gathering overseas is less visible and subject to fewer legal constraints than collection at home, in that it is beyond the reach of domestic laws and is likely to contravene the spirit and the letter of international law and the laws of other countries (Gendron, 2005, p.399).*

Gendron’s perspective proved to be a controversial issue that British intelligence grappled with during its military and counterintelligence operations in Northern Ireland. With one hand, the British army had a great desire to crush the IRA insurgency. With the other hand, Britain had to contend with the issue of legality and morality seen as Northern Ireland was still a part of the UK. David Charters has commented on the predicament of balancing domestic and international standards during counterinsurgency campaigns in far-flung regions of the British imperium. Put eloquently by Charters:

*The Army’s counter-insurgency doctrine, evolved over 25 years of fighting insurgency in the Empire, was difficult to apply in Ulster because the doctrine was not designed for domestic use ...harsh measures which had made a successful campaign possible in Malaya could not be applied readily in Britain, with its long traditions of individual liberty and freedom of the press. In Malaya, thousands of miles from home, operations beyond the jungle fringe could be conducted in almost complete secrecy; in Ulster, the daily movements of a patrol may be seen on TV that evening, in Belfast and in London (1977, p.25-26).*

Intelligence and subversive operations were thus under far less scrutiny in Malaya because of the simple fact that Malaya is not London or Belfast. The latter is far more important to British lawmakers, the public and the government than Malaya. At this stage

of the debate, the fundamental point to be made is that intelligence and ethics within a democracy are challenging to manage because intelligence and security forces often view foreign nations with lower concern and standards. It is therefore tricky to suddenly raise the norm when the doctrine is systemically rife with a lack of concern for privacy and to some extent, civil liberties of foreign citizens.

---

## 4.9 Media and Intelligence

---

In spite of the vast literature that has been scrutinised thus far, little focus has been attributed to intelligence and the media. The media can have a significant impact on keeping intelligence services in check, by exposing scandals. This was the case in 2013 when Greenwald revealed, (on behalf of Snowden) troves of information that demonstrated the extent to which GCHQ, NSA and its Anglo Five Eyes members were guilty of conducting surveillance across the globe in the name of national security (Borger, 2013). Conversely, media outlets can be guilty of singing off the same hymn sheet as intelligence services.

Although it is beneficial for media outlets to receive information from intelligence services, there is no guarantee that what is provided is objective and truthful. Once false intelligence is circulated, media outlets are guilty of damaging democracy despite their role of promoting it. Damien Van Puyvelde asserted a similar point indicating that ‘[i]ntelligence agencies and their political masters can also use the media to communicate on and justify intelligence activities’ (2014, p.288). Similarly, Matei has suggested that:

*An intelligence agency may utilize media outlets to convince the citizenry that its actions will achieve the policy goals drawn by the elected officials...If the media cover democratic reform of intelligence positively, they may show citizens that the agencies are trustworthy (Matei, 2014, p.84).*

Moreover, Hillebrand construed a similar perspective concerning the build-up to the second Gulf War in which the USG ‘would feed cooperative journalists with certain information, only to later refer to that publication to Legitimize its actions’ (2012, p.700). While journalists may feel that they are doing their job, they are actually doing the bidding

for rogue states that are seeking to conjure public support for acts of aggression abroad. For this reason, it would appear integral to check the validity of information to prevent entire nations from being fed government lies and exaggerations.

---

## 4.10 Privacy and Intelligence

---

Surveillance targets of the state need to eat sleep drive get on trains and do other daily activities as everyone in society. People of interest integrate with society and blend in so as not to arouse suspicion. As a result, surveillance is dispersed throughout society. However, the issue of privacy revolves around demarcating out zones of private spaces while still allowing intelligence services to operate efficiently. Put bluntly by Omand ‘[t]he realm of intelligence operations is, of course, a zone to which the ethical rules that we might hope to govern private conduct as individuals in society cannot fully apply’ (2009, p.9). In other words, intelligence and ethical concerns are an oxymoron, since operatives will at some stage need to penetrate the zone of privacy that is shared by many.

Ross Bellaby has also espoused a similar stance by construing the concept of privacy in terms of boundaries (2012, p.103). Accordingly, ‘[b]oundaries mark out areas where outside intrusion is unwelcome’ (Bellaby, 2012, p.103). An invisible yet paradoxically indelible line is present in which behind this line lies sensitive information, activities or possessions. Moreover, Bellaby has provided insightful analysis concerning privacy violations with regards to the individual’s lack of ‘autonomy’ concerning his/her ability to provide consent to intelligence sweeps:

*[B]y intercepting another’s communications, their privacy is violated. This is because, first, the activity involves intercepting and utilizing without consent information that is essentially the individual’s property, and second, by violating a sphere with a strong expectation that the individual is ‘in’ private, represented by the clear distinction between the ‘inside’ of the communication where the message exists and the ‘outside’ where the rest of society exists (Bellaby, 2012, p.104-105).*

For some, surveillance does not begin when a human has actually observed content, but at the moment when the collection has taken place. Cognisant of the fact that some



intelligence services in different parts of the world have the capacity to begin harvesting data from populations that are stored for longer than it should be, it is of no surprise that a portion of society takes the view that surveillance starts at the point of collection. The possibility of data being inspected is enough to convince people that surveillance starts at the point of collection as a result of public concerns (surrounding surveillance) in conjunction with scandals that have shown that intelligence services do not always abide by the rules. Proponents of Bellaby's view such as Paul Bernal have stated that:

*[T]he question of whether data gathering or algorithmic analysis constitutes 'surveillance' is largely a semantic point. Many of the key risks occur when data are gathered – the existence of data creates the risk. As a consequence it is at the data-gathering phase that the first privacy invasion occurs, regardless of whether that phase is described as surveillance or not (2016, p.249).*

On the contrary, to a degree it could be argued that intelligence gathering does not include 'doing things to people' however there is a great deal of psychological sensitivity when one considers the idea that another person or an elite organisation is watching citizens (Herman, 2004, p.342). In light of this stance, Bellaby has focused on the immaterial aspects of privacy violations concerning surveillance, announcing that:

*Even if the individuals are not aware their privacy is being violated, they are still 'harmed' insofar as their vital interest is wronged. For example, a camera inside an individual's home constitutes a violation of privacy and it can be argued that harm is done even though s/he might not experience the violation in a tangible or material way. Therefore, for intelligence collection, the interest in privacy features heavily in the debate over the right to be able to communicate in private, access the [I]nternet in private, control personal information and live in a house free from outside observation (Bellaby, 2012, p.103-104).*

This raises an incredibly contentious debate with regards to communications data. Back in 2015, the UK government highlighted that communications data only includes the, 'who, where, when and how of a communication but not its content' (Home Office, 2015[a]). A journalist may not want an intelligence service to know who they have been speaking with for the sake of confidentiality. Ironically, investigative journalists are the

ones who are supposed to be keeping democracy in check by highlighting wrongdoings by the government, keeping people informed about domestic and foreign affairs and placing the elite under legitimate public scrutiny. This role is greatly diminished if intelligence services can verify the sources of investigative journalists. Overall, it would appear that no matter what angle intelligence is explored from, issues surrounding ethics continue to appear. A state will never entirely sacrifice its security for the sake of ethical concerns. On the other hand, most democratic countries will never completely abandon the privacy concerns of its citizens for the sake of fulfilling aggressive demands from intelligence services.

---

## 4.11 Democracy and Propaganda

---

Both propaganda and democracy are well-researched areas that have produced a significant body of scholarship irrespective of whether they are viewed separately or in unison. A litany of critical academics have been drawn to the flame of propaganda and democracy primordially due to the utility of the former within a democracy. To begin with, it is vital to define and explore both terms to identify why some academics have shown interest in this research area. Firstly, in the view of Geroge Catlin democracy is described as a ‘system of government under which the executive and the majority of the legislature are, at regular intervals, elected by the majority of the citizens, or by the largest single group, and are accountable to it’ (1935, p.219). Citizens have the privilege of choosing who their leaders are whereas under a dictatorship those that are in power tend to keep power for themselves or others that they have chosen. Within a democracy, Mitchell Dean has asserted that decision making and governing requires:

*[A] multiplicity of authorities and agencies, employing a variety of techniques and forms of knowledge, that seeks to shape conduct by working through our desires, aspirations, interests and beliefs, for definite but shifting ends and with a diverse set of relatively unpredictable consequences, effects and outcomes (Dean, 2007, p.11).*

Although people are free to make decisions within the given confines of the law, perception in a democracy is managed and influenced as a form of ‘governmentality’ to ensure that government policies are maximised (McKinlay, Carter and Pezet, 2012, p.3-

5). Dean's assessment of governmentality suggests that 'those who seek to govern, human conduct is conceived as something that can be regulated, controlled, shaped and turned to specific ends...government of these things involves the attempt to shape rationally human conduct' (2007 p.11). The next topic in focus, propaganda, has come to be defined in quite a negative light to which a propagandist is seeking to dupe an unwitting public. Propaganda is associated with propagating anti-rational ideas which appeases pre-made stereotypes. Brown has rightfully asserted the view that:

*[T]he fundamental mechanism employed by all forms of propaganda is, as we have seen, suggestion, which may be defined as the attempt to induce in others the acceptance of a specific belief without giving any self-evident or logical ground for its acceptance, whether this exists or not* (Brown, 1963, p.25).

On the other hand, when does propaganda stop being denoted as propaganda and referred to as education? In other words, regardless of an ulterior motive, the presentation of the truth can be viewed by an opposition group as an uncomfortable inconvenient truth; therefore, labelled as propaganda. In the case of Japanese *Negro* propaganda during WW2, a sizable amount 'of the propaganda released during the war...did not need to rely on fabrication. Propaganda often depicted the actual situation in the US: lynchings, discrimination against Blacks and other minorities, Jim Crow laws' (Masaharu, 1999, p.6). With this case in mind, was Japanese information directed towards African Americans worthy of being deemed anti-rational propaganda?

Coincidentally, Japanese narratives were at the heart of Malcolm X's black nationalist ideology and general African American resentment towards the notion of fighting in American wars without justice being delivered to African Americans in the US (Malcolm X, 1963, cited in University of Virginia, 2003). Perhaps in the mind of US policymakers, Japan was not interested in educating African American's or any group in America for that matter. The intent was apparent, and that was to cause social tension with groups in the US that endured inhumane treatment for centuries (Masaharu, 1999, p.9).

Furthermore, it is essential to note that not all propaganda messages are inherently distasteful. In fact, propaganda has been used for 'advertising with the intention of stimulating trade' (Catlin, 1935, p.220). Similarly, propaganda slogans such as *jobs now* were used by African American protestors during the civil rights marches. In the case of

fighting for women's rights, during the 20<sup>th</sup>-century propaganda was a crucial weapon that helped to stimulate discussion on social inequalities (Bernays, 2005, p.129). On the other hand, Robert Jensen has pointed out that the emergence of a mediatised 'pornography-saturated culture in which women are routinely targets of sexual violence and intrusion' has made pornography in the US a 'form of propaganda for rape culture' (2011 p.159). From Jensen's perspective propaganda in this particular context is paraphernalia for a degenerate culture that oppresses women.

Definitions of propaganda tend to orientate around deception and the desire of a propagandist to convey negative messages. For example, according to William Biddle '[p]ropaganda becomes a process of wholesale emotional conditioning, outside the knowledge of the subjects' (1931, p.294). Similarly, propaganda is also described as 'the fabrication and diffusion of messages that distort facts and induce misinformation for the purpose of advancing government interests' (Castells, 2009, p.264). In light of this definition, Western nations attempt to erect an ontological barrier between themselves and propaganda to emphasise how antithetical this sullied form of communication is to the foundations of democratic governance.

Despite the damage caused by propaganda in WW1, the late Phillip Taylor expressed the view that democracies often erect a false notion that it is only un-democratic systems who wield propaganda. According to Taylor, the 'democratic myth that propaganda is something conducted only by someone else, usually by an (undemocratic) enemy or potential adversary, and that it is about untruth' (2002, p.437). It is this very myth that made '[o]fficial spokespersons working for democratic governments...nervous about having their work described as "propaganda"', for fear of becoming precisely what they incessantly and vehemently repudiate (Taylor, 2002, p, 437) (see chapter 6 and 7).

Despite egregious efforts by governments to distance themselves from propaganda, its use is viewed as fundamental to democracy. In the view of Eric Louw '[o]ne of the dimensions of mass democratic politics is hype making. Just as magicians use smoke and mirrors to distract their audiences and conjure up illusions, so too does the political machine and its media staffers' (2005, p.143). Irrespective of whether or not propaganda and democracy are two fundamentally different elements, literature so far suggests that the former benefits the latter as well as the latter benefiting the former. While democratic

systems struggle with accepting that they are in the business of propaganda, some have assumed that utilising propaganda is not such a bad idea if a country wishes to withstand ideological threats from its adversaries.

Catlin boldly suggested that '[t]he dilemma of democracy is that the democrat, as tolerant, must concede to these people the right to their own convictions', which in many respects leaves the system of governance open to attacks by propagandists from opposing systems (1936, p.134). Taylor also pointed to the utility of propaganda as a means to promote and keep democracy resilient from adversaries that wish to subvert it. In other words, while 'democracies tend to delude themselves that they are not in the business of propaganda ... governments need to conduct international information campaigns—which some may call propaganda—to ensure that their “truth” prevails' (Taylor, 2002, p.437). This point is correct with regards to the aftermath of the Korean War. According to Young Lim and Jennifer Lemanski, South Korea responded to North Korean communist propaganda with large 'speakers, sending messages of the superiority of democratic systems to communism' (2017, p.161).

Similarly, during the outbreak of war in 1939, allied propaganda portrayed the war against Germany as a fight to protect democracy and humankind (Ibhawoh, 2007, p.238). Propaganda is thus essential to repelling ideological attacks particularly during or shortly after a nation has been at war. In light of this viewpoint, propaganda, to some extent is a rather benign activity as opposed to a truculent, sneaky reprehensible tool. This stance resonates well with Joseph Roucek opinion on the issue, who previously highlighted that propaganda is a chief defence against antidemocratic forces and their lies (1956, p.408).

Furthermore, Taylor has suggested that facts should not be left to speak for themselves but explained to avoid manipulation by nefarious undemocratic actors (Taylor, 2002, p.439). In a free democratic space where access to the outlandish lies on the Internet is possible, can the average citizens be left to their own devices to realise the correct conclusion? This question bears a heavy burden on public opinion, which to some policymakers may be a dangerous gamble. Considering that, '[p]ropaganda, with all its protean variety, its lurking interlinear presence, and slick visual appeal demands a special repertoire of communication talents to recognize and respond to it', it may be viewed as

chimerical to assume that an unwitting public can be left to figure things out which were crafted in the shadows by foreign intelligence services (Cunningham, 2001, p.146).

Understandably few politicians would risk their political career by openly undermining the intelligence of his or her constituents. In any case, the underlying issue remains at large; are citizens wise enough to withstand propaganda from adversaries? (see chapter 7). Contemporary research from Phillip Howard and Bence Kollanyi on computational propaganda has also in part lent support to Cunningham's assumption stating that '[i]ncreasingly, political campaigns automate their messaging and many citizens who use social media are not always able to evaluate the sources of a message or critically assess the forcefulness of an argument' (2016, p.5). Public opinion equates to power in a democratic society in which politicians rely on voters. Therefore, it is not inconceivable to assume that this power base must be protected and in some cases, managed. Lasswell pondered the notion of democratic governments managing the perception of its citizens in stating that:

*Thus argues the despondent democrat. Let us, therefore, reason together, brethren, he sighs, and find the good, and when we have found it, let us find out how to make up with the public mind to accept it. Inform, cajole, bamboozle and seduce in the name of the public good. Preserve the majority convention, but dictate to the majority!* (Lasswell, 1972, p.5).

In essence, the public mind is something to be managed as opposed to hoping that citizens can independently gravitate to the right democratic principles. During the early 20<sup>th</sup> century this viewpoint was not particularly unique amongst commentators. According to Miller, early 20<sup>th</sup> century scholars such as:

*Gustave LeBon, Graham Wallas and John Dewey... Lippmann... arrived at the bleak view that "the Democratic El Dorado" is impossible in modern mass society, whose members – by and large incapable of lucid thought or clear perception, driven by herd instincts and mere prejudice, and frequently disorientated by external stimuli – were not equipped to make decisions or engaged in rational discourse* (Miller, 2005, p.16).

Consequently, to keep society and the public opinion running as smoothly as possible, '[t]he conscious and intelligent manipulation of the organised habits and opinions of the

masses is an important element in democratic society' (Bernays, 2005, p.37). Moreover, Lippmann, in particular, questioned the overall capability of the average citizen to engage in democracy successfully. In the book *Public Opinion*, Lippmann juxtaposed the likelihood of an 'omnicompetent citizen' existing in a 'rural township' as opposed to a sophisticated bristling city (1997 p.173). Due to the enclosed and integrated network that generally exists in a rural town, '[e]verybody in a village sooner or later tries his hand at everything the village does. There is rotation in office by men who are jacks of all trades' (Lippmann, 1997, p.173). A familiar and truncated surrounding allowed citizens within this network to become deeply rooted in local affairs. In contrast, knowledge of foreign affairs was likely to be based on grossly inaccurate assumptions about a world that is unfamiliar to them.

Due to the proximity of local affairs, Lippmann indicated that citizens in rural towns were 'fitted to deal with all public affairs' and favourably 'endowed with un-flagging interest' (1997, p.173). Conversely, the ideal omnicompetent notion falls short when 'the democratic stereotype was universally applied' (Lippmann, 1997, p.173). To some extent, the average citizen in a bristling city, which is often impacted by globalisation and foreign affairs is ill-equipped to digest huge volumes of information. Albeit bleak and patronising, Bernays reinforces Lippmann's view, by imagining the burden that would be placed on the average citizen:

*[I]n practice, if all men had to study for themselves the abstruse economic, political, and ethical data involved in every question, they would find it impossible to come to a conclusion... if every one went around pricing, and chemically tasting before purchasing, the dozens of soaps or fabrics or brands of bread which are for sale, economic life would be hopelessly jammed (Bernays, 2005, p.38-39).*

Following this perspective, Lasswell has previously explored the possibility of genuine democratic rationality spreading by asking two fundamental questions:

*'What happens when this form of rationality spreads-when more and more people are prodded into the rational calculation of their special "interests"? Is it possible that the spread of rationality intensifies non-rationality, hence that it heightens the level of general insecurity?' (Lasswell, 1935, p.188).*

From this angle, it is possible that attempts at rational thinking and the contribution to governance by lay individuals can result in a societal disaster. Propaganda is to some extent a necessary instrument to truncate information into digestible units so that people have some form of understanding about the surrounding environment. Furthermore, there is a case to be made that the public consciously accepts propaganda and in some instances, desires a long-lasting relationship with the propagandist. Ellul presents the impression of a public that seeks the company of the propagandist who is not necessarily an enemy of the people. In the book *Propaganda: The Formation of Men's Attitudes* Ellul explains this point in a series of assertions, '[c]rowds, go mad when they no longer know what posture to assume toward a threat. Propaganda provides the perfect posture with which to place the adversary at a disadvantage' (1973, p. 159 - 160). This assumption prompted Ellul to suggest that:

*Contemporary man needs propaganda; he asks for it; in fact, he almost instigates it. The development of propaganda is no accident. The politician who uses it is not a monster; he fills a social demand. The propagandee is a close accomplice of the propagandist* (Ellul, 1973, p.160).

The conscious symbiotic unison between both the propagandist and the 'propagandee' highlights quite a rare depiction, in a way that justifies or at least, rationalises the existence of propaganda within a democracy (Ellul, 1973, p.160). Ellul's portrayal of this relationship would, therefore, justify Taylor's previous assertion that highlighted the utility of propaganda in a democracy (see chapter 7). So far, various academics have presented a strong case as to why propaganda may be necessary or even 'the type of coercion that peculiarly accompanies the growth of democracy' (Biddle, 1931, p.283). Biddle explained this assertion about propaganda in suggesting that '[l]ike democracy, it is dependent upon widespread literacy and rapid social communication, the telephone, the press, the radio, the motion picture' (1931, p.283). This connection will not sit well with democratic purists, but the literature covered so far provides insight into the potential necessity of propaganda within a democracy (see chapter 8).



---

## 4.12 Media as Propaganda Platforms for the State

---

Media outlets in democratic nations can consciously or unwittingly become loudspeakers for propaganda dissemination that deceives domestic and international audiences. The literature on propaganda techniques reveals that Western intelligence services during the Cold War covertly made use of media outlets (Cullather, 1997, p.63-64; Agee, 1975, p.121). In particular, according to Tony Shaw, the IRD ‘distributed material to Asian media contacts’ during the Korean War in the early 1950s (1999, p.278). Throughout the Cold War, the IRD took part in an international propaganda campaign to help counter communist narratives that were harmful to the interest of the UK and her allies. Research by Shaw has suggested that the IRD’s approach to providing non-attributable propaganda to media outlets garnered a negative impression amongst the public and mass media about communism (1999, p.280).

Furthermore, David McKnight has shed light upon the Australian Security Intelligence Organisation (ASIO) that engaged in ‘spoiling operations which were interventions designed to disrupt the political advance of the left, especially the Communist Party of Australia (CPA)’ (2008, p.6). Spoiling operations consisted of Australian intelligence operatives initiating contact with journalists in order to suggest stories favourable to the ASIO (McKnight, 2008, p.10). Moreover, there is no shortage of academic commentators that have scrutinised the media’s role in exonerating propaganda during the Second Gulf War (Gunter, 2009, p.42-43; Ryan and Switzer, 2009, p.46-48; Kellner, 2004, p.329-333; Paolucci, 2009, p.863-865). To be specific, the literature on propaganda that was disseminated by the Bush Administration and Western media appears to be nearly unanimous in condemnation of how information was contorted.<sup>7</sup> In light of this viewpoint, Peter McLaren and Gregory Martin have suggested that:

*Media lies, in the form of spin manoeuvres and disinformation campaigns, must be understood as part of a domestic psyop (psychological operation) aimed at producing ideological oxygen for Bush’s war on Iraq and building support for any future adventures (McLaren and Martin, 2004, p.287).*

---

<sup>7</sup> I am referring to George W. Bush, not George H. W. Bush.

Without an auxiliary information medium such as the media to transmit the Bush administration's point of view, convincing the US population about the necessity to go to war may have been difficult. Deepa Kumar has reinforced McLaren and Martin's narrative, highlighting that '[t]oday, few would disagree that the Bush administration resorted to propaganda to justify its war on Iraq and that the news media simply presented as fact information that they should have carefully scrutinized' (2006, p.48). While the media is a crucial part of democracy; the second Gulf War is a perfect example of the media's obedience towards state-driven narratives.

Techniques have developed to make propaganda efforts in conjunction with the media appear less secretive and more natural. Propaganda and the use of embeds or more formally known as embedded journalism has become a prominent theme in the 21<sup>st</sup> century particularly during the second Gulf War (Johnson and Fahmy, 2009, p.52-54; Kumar, 2006, p.60-61; Pfau et al., 2005, p.469). Embeds are journalists that have 'agreed to give up most of their autonomy in exchange for access to the fighting on military terms' (Miller, 2004, p.89). Despite the extensive use of embeds by the US military, '[j]udgements about the embed programme are ambiguous' (Brandenburg, 2007, p.956). David Miller has indicted that embedding journalists is a propaganda manoeuvre 'dreamt up by the Pentagon and Donald Rumsfeld' which seeks to espouse positive messages and control what is reported (2004, p.89; Fahmy and Johnson, 2007, p.98). At this stage, it is clear to see that the media is inexorably bound to propaganda, even in some of the most democratic nations in the West. Embeds can play a vital role in providing viewers with rare footage of warfare; however, it may come at a detrimental price to democracy and the truth.

---

## 4.13 Control

---

Propaganda has developed as a necessary tool to help democratic states overcome their former tendencies to use force as a means of social control. Contemporary academics such as Florian Zollmann have proselytised a similar stance in highlighting that '[w]ith the ascendancy of liberal democracy; propaganda was instituted to govern people through the management of perception and behaviour' (2017, p.331). Furthermore, according to

Dodge '[t]he expansion of propaganda to political fields was directly conditioned on the growing power of public opinion in government' (1920, p.241).

In other words, as politicians became more aware of the increase in education throughout the population in which they depended upon, propaganda became a necessary tool to push public opinion in any favourable direction. Similarly, Chomsky suggested that '[t]he logic is clear. Propaganda is to a democracy what the bludgeon is to a totalitarian state' (2002, p.20-21). The control factor is thus woven into the power of propaganda, albeit in a less raw and apparent form than the bludgeon. Although fear is still necessary for a democracy and law enforcement agencies, propaganda has effectively become an integral tool to wield against the public. Accordingly, Dean's assessment of governmentality has suggested that 'those who seek to govern, human conduct is conceived as something that can be regulated, controlled, shaped and turned to specific ends...government of these things involves the attempt to shape rationally human conduct' (2007 p.11).

Furthermore, Roucek described propaganda as the 'deliberate effort to control the behaviour and relationships of social groups through the use of methods which affect the feelings and attitudes of the individuals who make up the groups' (1956, p.408). This stance is accentuated further in the fact that Lasswell previously defined propaganda as a 'technique of social control' (Lasswell, 1935, p.189). This definition has stood the test of time, as Chomsky's assessment of democracy and propaganda complements Lasswell's description. Moreover, Chomsky has highlighted the perspective of a government in stating that society is embroiled in a constant struggle in which '[t]he bewildered herd never gets properly tamed' (2002, p.32).

Fearful of 'segments of the population...becoming organized and active and trying to participate in the political arena' during '[t]he crisis of democracy' (Chomsky, 2002, p.33). The modern democratic state needs to act with force but ideally without excessively aggressive acts. In the absence of force, citizens may feel emboldened to challenge state authority or meaningfully participate in democracy. Accordingly, the 'population has to be driven back to the apathy, obedience and passivity' by shaping and forming perception (Chomsky, 2002, p.33).

On the other hand, regardless of the compelling literature amassed above, the extent of human agency amidst propaganda is still debatable. Although propaganda has had a noticeable effect on people's lives; it may be too simplistic to assume that the modern human is unequivocally controlled by propaganda. Cunningham suggests a similar view: '[i]t seems like an exaggeration to claim that propaganda robs us of our freedom and turn us into automatons, yet it certainly sets impediments in our way, thereby inhibiting our capacity to know and to act well' (2001, p.139). Perhaps Brexiteers chose Brexit because they long to be rid of the EU's authority and shared identity as opposed to being victims of a dirty propaganda campaign by unscrupulous Conservative MP's and Dominic Cummings. Propaganda and control indeed have close ties, but it is debatable to assert unequivocally that humans are slaves to propaganda.

---

## 4.14 Robot Trolling and Modern Methods of Propaganda

---

Amongst the plethora of modern online tactics that are used to warp perception, a considerable amount of academic interest focuses on automated or semi-automated bots which spread propaganda. This has been referred to as computational propaganda by researchers associated with Oxford University's COMPROP (Howard et al., 2017, p.1; Gallacher et al., 2017, p.1). Computational propaganda is best described as the 'automated dissemination of fake news, misinformation propaganda and other forms of junk news' (Neudert, Kollanyi and Howard, 2017, p.1). Bots can be used for benign purposes, such as calculations (Khanna et al., 2015, p.277). On the other hand, bots are also used to spread propaganda in cyberspace (Howard et al., 2017, p.1).

Research on coordinated computational propaganda during state elections have produced different outcomes, which raises questions as to how much of an impact bots can have on public opinion. Howard and colleagues research on junk news discovered that computational propaganda had a sizable presence online during the 2016 US presidential election (Howard et al., 2017, p.1-4). On the other hand, computational propaganda has had less of an impact in different regions of the world. Research concerning computational propaganda during the UK general election discovered that 'automated

accounts generate a relatively small amount, 12.3%, of the total content being shared about the UK election' (Gallacher et al., 2017, p.5). The available literature on computational propaganda has not produced a significant amount of evidence to suggest that public opinion throughout all of Europe is facing an irreversible existential crisis. However, Howard and Kollanyi have indicated that '[b]ots have been used by political actors around the world to attack opponents, choke off hashtags, and promote political platforms" thus becoming a useful online platform for shaping opinions (2016, p.5).

To conclude, the literature on propaganda and democracy seem inexorably bound to each other, in a way that the former complements the latter. It would seem ludicrous to assume that democracy can be left open and defenceless against external forces without the democrat rushing to defend his or her system. However, this does raise a controversial issue of morality that is highlighted in Chapter 5, 6, 7 and 8. Overall, propaganda and democracy help each other to develop exponentially. To ignore this would be to ignore how democracy has managed to defend itself from communism during the Cold War.

---

## Chapter 5 Case Study 1: Propaganda, Surveillance and Ontological (In) Security a Case of West vs the East

---

Throughout the Cold War, the US and its Western allies were locked in an information battle against the Soviet Union (NATO, 1953, p.2). Knowledge of Soviet propaganda campaigns against NATO caused enough OIS amongst its NATO members that they created an Information Working Group to counter Soviet information to bolster NATO's claim of relevance to the world as a fundamental organisation (NATO, 1952, p.1-2). Since the end of the Cold War, both camps have maintained hostilities towards each other which have included intelligence and propaganda operations. In this section, I maintain the claim that attempts to mitigate OIS in the field of cyber propaganda only serves to create additional OIS (see chapter 1 and 3). Thanks to the Snowden leaks, it has been revealed that British intelligence services (GCHQ and JTRIG) attempted to warp perception throughout the world by using social media platforms to inject propaganda in cyberspace (see chapter 1).

This revelation came about in 2014 and again in June 2015 (see chapter 1). However, the actual operation to begin warping perception overseas stretches back to 2011 (see chapter 1 and 3). Attempts by GCHQ to warp perception abroad through cyberspace as a means of placing Britain in a favourable global position, signalled to other nations that online propaganda is a serious international endeavour. On the topic of Russian cyber interferences, MI5 has told the UK Intelligence and Security Committee in 2017 that Russia is clearly 'operating to risk thresholds which are nothing like those that the West operates' (Parliament. House of Commons, 2017, p.59). While there is an element of truth to this claim, British intelligence services must look honestly at the Snowden leaks which exposed JTRIG's list of cyber dirty tricks.

Since the Snowden leaks, many states have replicated JTRIG's tactics (see chapter 1). In the case of Russia's replication of JTRIG tactics which included the use of false personas to sow dissent during the US 2016 elections, a significant amount of OIS left portions of the USG bitterly divided between party lines of Republicans and Democrats (Pew Research Center, 2017; Bloomberg Politics, 2018). Although it is true that discourse surrounding the US 2016 election is not predicated on British intelligence services,

international competition and willingness to use JTRIG's tactics has increased since GCHQ's propaganda endeavours were leaked. Realist competition between nations that perceive each other as strategic threats often results in countries or alliances increasing defensive and offensive military and intelligence operations.

The context of a modern increase in cyber dirty tricks between states needs to be viewed as WW2 and post WW2 desire to develop and use nuclear weapons. Once the US developed the atomic bomb, other great powers such as the Soviet Union, the UK, France, China, Pakistan, India, South Africa, Israel and others became eager to possess such a destructive weapon. In a similar light, once it became clear to the world in 2014 and 2015 that GCHQ was prepared to use social media platforms to inject propaganda via fake personas and target multiple nations with dirty tricks, Russia and other states followed suit (see chapter 1). The physical damage caused by nuclear arms has created a considerable amount of restraint among nations who possess them. On the other hand, in most cases, online propaganda does not immediately produce physical harm. Therefore, states have begun covertly shaping perception online.

Although gunboat diplomacy is still a prominent theme, particularly for global powers that possess aircraft carriers and naval destroyers, propaganda and surveillance have become two prominent tools to shape foreign affairs. Covert propaganda and surveillance campaigns are difficult to attribute to a state, whereas gunboat diplomacy is readily identifiable. Therefore, in the modern era, dirty tricks campaigns are just as readily available as gunboat diplomacy. Moreover, Britain's willingness to use online propaganda has raised the threshold of other nations who wish to shape the perception and foreign policy of other nations. Great power nations such as Russia are merely keeping up with great power capabilities to shape perception throughout the world.

While it is difficult to unequivocally prove that Russia has pre-emptively engaged in vast propaganda and surveillance campaigns against the US, let alone as a result of leaked JTRIG slides, what can be said is that the latter may have indeed ruptured Russia's sense of self and security in cyberspace. As a result, Russia and other states have increased their threshold to that of GCHQ, against Western states such as the US. Following this line of thought, this chapter suggests that JTRIG's efforts to secure British OIS has encouraged other states to follow suit. Attempts by Britain to secure its position globally and to

mitigate OIS has directly or indirectly resulted in the US enduring OIS as Russia test-fired JTRIG's tactics on an international scale.

To a great extent, Britain's motives that have been acted out through GCHQ are a continuation of its information endeavours that were previously executed by the IRD during the Cold War (see chapter 3). Moreover, this chapter will outline the importance of OIS amidst a propaganda and surveillance campaign that has targeted a Western state. I will juxtapose JTRIG's methodology of dirty tricks with how the US election was allegedly targeted by Russia, with similar measures. This will be done, by highlighting and discussing the responses of Senators from the Democratic Party and Republican Party.

---

## 5.1 JTRIG, Russia and the US 2016 Presidential Elections

---

Taking into account Britain's historical background in propaganda (see chapter 3), multiple states such as Russia may have experienced what some academics refer to as OIS (Kinnvall and Mitzen, 2017, p.3-6; Mitzen, 2006, p.345) (see chapter 2 and 4). On the other hand, during the US 2016 presidential elections, JTRIG's playbook of online dirty tricks was emulated and weaponised by a hostile actor that the USIC has named as Russia (ODNI, 2017[b], p.6). While it is difficult to draw a definitive link between the release of British propaganda efforts against Russia and its (Russia) alleged involvement in the US 2016 election, it is of no surprise that Russia Iran and other nations have begun emulating JTRIG's playbook. As such, the threshold for retaliation has increased potentially due to fear and OIS amongst the West's adversaries who are aware of the Snowden leaks concerning JTRIG.

As early as 2015, the USIC was aware that hackers of Russian origin had hacked into the Democratic National Committees IT systems (Sciutto, 2017). The DNC was the victim of a simple but effective spearfishing campaign. One-click of a malware-laden email by Hillary Clinton's presidential campaign manager John Podesta, gave Russian hackers a



free hand to inspect and exfiltrate sensitive information from the DNC (Nakashima and Harris, 2018). Sensitive information gained was given to WikiLeaks.

Highly controversial information that appeared to show the DNC's favouritism towards Clinton at the expense of Democratic candidate Berny Sanders was exposed by WikiLeaks (WikiLeaks, 2017[a]). In fact, WikiLeaks has an entire section dedicated to Clinton which contains over 50,000 pages of documents (WikiLeaks, 2017[a]). Moreover, in 2017 Facebook's report on this matter uncovered evidence of an information campaign on its platform to sow division in the US. Internal investigations conducted by Facebook revealed '470 inauthentic accounts and Pages' that pushed out 3,000 ads (Facebook, 2017). Facebook has concluded that 'approximately \$100,000 in ad spending' was spent between June of 2015 to May of 2017 (2017). Ironically, the ads discovered by Facebook did not:

*[S]pecifically reference the US presidential election, voting or a particular candidate. Rather, the ads and accounts appeared to focus on amplifying divisive social and political messages across the ideological spectrum — touching on topics from LGBT matters to race issues to immigration to gun rights (Facebook, 2017).*

Concerning the source or origin of the propaganda and surveillance campaign, Facebook's internal investigation has indicated that 'these accounts and pages were affiliated with one another and likely operated out of Russia' (Facebook, 2017). Even though senior US political figures such as Senator Warren conceded to the notion that the DNC was 'rigged' against Sanders in favour of Clinton during the 2016 election, America was divided over the motive behind the leaks against Clinton (CNN, 2017[a]). On the other hand, the USIC and government figures have taken a more aggressive and hostile tone towards Russia, to which I will demonstrate is a result of OIS.

During and after the US 2016 presidential election, candidate and now President Trump continued to play down and contradict the USIC assessment concerning Russian meddling (Trump, 2018, cited in BBC, 2018[b]). President Trump's unwillingness to form a policy against Russian interference angered various Democratic Senators. Although a litany of Democrats and Republicans have accused Russia of interfering in

the US 2016 elections, the discourse of three government figures, in particular, i.e. Senator Warren, Senator Swalwell and Senator Warner, displayed signs of OIS during interviews.

Simultaneously, futuristic depictions were ironically presented to heighten a sense of anxiety, a fractured American identity and national security concerns as a means of stitching together a sense of OS. In order to affect policy change within the Trump administration, I argue that Democratic Senators were willing to work towards plunging America's sense of OS in order to use America's depleted sense of self as a bargaining chip to seek a unified response as it has done in previous wars. President Trump's cantankerous response that refused to blame Russia for interference encouraged Democratic Senators to construe narratives predicated on alarm, division and weakness to force a policy change.

The US has been involved in several skirmishes small conflicts and large scale wars throughout the 19<sup>th</sup>, 20<sup>th</sup> and 21<sup>st</sup> century. Conditioned by the Realist anarchic environment that has enabled the US to use its armed forces in foreign adventures; in times of conflict, America is accustomed to a unified ontological response that addresses its resolve to fight various adversaries. After Japan's air raid on America's naval fleet in Pearl Harbour Hawaii, former US President Roosevelt's declaration of war speech highlighted the extent of damage inflicted by Japan. Simultaneously, President Roosevelt reassured the nation of complete victory and future safety. According to President Roosevelt:

*The attack yesterday on the Hawaiian Islands has caused severe damage to American naval and military forces... Yesterday the Japanese Government also launched an attack against Malaya. Last night Japanese forces attacked Hong Kong: Last night Japanese forces attacked Guam. Last night Japanese forces attacked the Philippine Islands...As Commander in Chief of the Army and Navy I have directed that all measures be taken for our defense...No matter how long it may take us to overcome this premeditated invasion, the American people in their righteous might will win through to absolute victory (Library of Congress, 1941).*

Similarly, at the precipice of hostilities between Iraq and US forces, President Bush went on to construct a sense of conviction, unity and assurances in a victory against a distant adversary (Iraq):

*My fellow citizens, the dangers to our country and the world will be overcome. We will pass through this time of peril and carry on the work of peace. We will defend our freedom. We will bring freedom to others. And we will prevail. May God bless our country and all who defend her* (Bush, 2003, cited in CNN, 2003).

The confidence to step forth into an anarchic international arena was reinforced by narratives of unity and the resolve to vanquish those who have disrupted America's sense of security. In the case of the 2016 US presidential election interference, ontological unity was absent despite prominent Republican Congressman John McCain suggesting that Russian meddling was an act of war (McCain, 2016, cited in Walsh, and Schleifer, 2016). TheUSIC highlighted the threat from abroad, but customary narratives that previously allowed the US to pivot to a safe space before stepping forward into anarchy was missing (ODNI, 2017[b], p.6). This void left US Democratic Senators in a state of OIS. In order to mitigate the feeling of personal and national OIS, Democratic Senators attempted to plunge America's sense of OIS into further crisis in a desperate attempt to induce customary narratives from President Trump that would unify the country against Russian dirty tricks.

---

## 5.2 Senator Eric Swalwell

---

In the case of Senator Swalwell, it was clear that the effects of OIS had permeated his world view post-2016 election. According to Senator Swalwell '[l]ast election, Russia attacked our democracy, infecting us with a virus we have still not kicked' (Swalwell, 2017). Senator Swalwell has depicted America as a victim of an infection while emphasising the notion that it has not been dealt with. From one angle, this potentially leaves the mind open to the risk of further damage, which would in turn, encourages readers to ponder why this virus has not been removed.

This conundrum thrusts the intended American listener into a potential state of OIS due to being exposed to temporarily unanswered questions concerning the stability and sovereignty of US democracy. Keeping in touch with the notion of the state and OS,

Kinnvall has presented her interpretation of OS by asserting that '[f]rom an ontological security perspective focused on state narratives and actions, resentment is intimately connected to anxiety and fear – anxiety in terms of losing national control in the face of the state' (2017, p.95-96).

This conception of OS reinforces Senator Swalwell's concern of American sovereignty since a virus, usually hampers a host's ability to act. Senator Swalwell is, therefore, trying to emphasise the gravity or severity of this attack by employing the metaphor of a virus, which in turn sheds light on his sense of OS and lack of agency to react. With this virus in mind, it is likely that Swalwell does not see peace and stability in cyberspace as something that Americans can enjoy, in part due to USG's unwillingness to deal with the Russian threat.

However, Senator Swalwell employs the security-seeking strategy of carving out OS through making future stability conditional on discursive homogeneity. Accordingly, '[t]he only antidote to a future attack is unity in identifying how we were so vulnerable and who was responsible' (Swalwell, 2017). At this point, it is clear that Senator Swalwell is seeking to rally US citizens around him to produce a homogenous identity that can confront an issue as opposed to being an isolated, fragmented voice that is drowned out by a cacophony of counter-narratives and possibilities in cyberspace. Senator Swalwell is attempting to forge a sense of OS in order to secure or reset his sense of Americanism to rebuff what he sees as a foreign incursion into the very fabric of American democracy. At this juncture, it is evident that Senator Swalwell's attempts to render his initial statement concerning the Russian virus as inadequate, through the emphasis of unity. When nations are faced with adversity concerning intelligence threats, stitching together some form of a unified front is integral.

The 2016 election interference is different from Japan's Pearl Harbour attack, which was clearly attributable, allowing the US to unite ontologically and take action physically. In cyberspace, the context is different. Nations can have contradictory selves. That is, with one hand diplomats can insist they have nothing to do with an attack, while his or her intelligence services are operating in cyberspace to launch propaganda and surveillance campaigns. Due to the inability to be sure of an attack in cyberspace America's OS is

pegged to percentile estimations of who was responsible for the US 2016 interference. Ontologically, the US is divided and unable to collectively pivot to a safe place of rehearsing familiar anarchic Realist roles because it is unsure of the circumstances of the 2016 election interference.

---

### 5.3 Senator Mark Warner

---

Senator Warner, an outspoken critic of Russia, presented a reality in which America was incapacitated or unable to react to the threat of alleged Russian interference due to President Trump's unwillingness to robustly condemn alleged meddling in the 2016 US presidential elections. According to Senator Warner, '[w]e've got to be ready in 2018... the one thing we've heard consistently is the Russians will be back, and Jake what bothers me is because the president won't acknowledge this attack, we don't have a whole government response' (CNN, 2017[b]). Concerning Senator Warner's response, the most poignant theme that is evident concerns the lack of agency to operate within an environment that appears to be permeated with risks from an external adversary (Russia). Senator Warner's frustration is that the current US administration and America (in general) will not be able to react efficiently to an enemy, thus leaving the US sinking in quicksand. This interpretation is synonymous with Mitzen's analysis of agency and OIS; '[w]hen there is ontological insecurity, the individual's energy is consumed meeting immediate needs. She cannot relate ends systematically to means in the present, much less plan ahead. In short, she cannot realise a sense of agency' (2006, p.345).

If Mitzen's interpretation is accurate, Senator Warner and other Americans cannot wield the means to bring about an end solution or government response. In reality, intelligence services work aggressively to thaw out attacks from malicious actors. However, without unilateral governmental support to confront Russia, the US will feel that it's Cold War adversary has gotten away with intervention and is poised to commit the act again. Without the agency to act as a whole nation that is united against a common foe, Senator Warner is unable to transform the means to a real solution.

At this juncture, it is essential to emphasise that OS is predicated on the notion that an individual or group of people can trust their sense of self to navigate through life despite how tumultuous the environment may be. Senator Warner's world view is fraught with

anxiety and a lack of OS because he is concerned that the Russians will strike again while the government is divided and unable to muster a significant response towards Russia.

Moreover, when speaking on information warfare at the Carnegie Endowment for International Peace, Senator Warner elicited more signs of OIS when stating that ‘[a]nd now this playbook is actually out in the open, and we have to worry about more than just Russia. These tools can be used by other actors– China, non-state actors, terrorists, and others to try to influence, and sow discord within our nation’ (Warner, 2018, p.7). Cognisant of the fact that the world has watched America spiral into a divided society as a result of alleged Russian interference, it is evident in Senator Warner’s speech that he is concerned that others might emulate the same formula in the near future.

In the case of propaganda, nations seek to envision and highlight their fears and enemies in the form of a list to map out the tumultuous terrain that they need to navigate. In doing so, Senator Warner can re-establish patterns and narratives that are more familiar to the overarching narrative of American security. This is a vital ontological and rhetorical tool due to the nature of covert propaganda. Amidst the inability to be unequivocally sure of the source of covert propaganda, people need to cast a shadow(s) on the wall for fear of staring at a blank canvass with no idea where or who the enemy is. Therefore, enumerating a list of potential enemies as Senator Warner has done ‘creates an illusion of predictability but prevents seeing other dimensions of the problem and leads to a known and well-rehearsed routine of policy escalation and popular suspicion’ (Chernobrov, 2016, p.584). In the field of cyberspace, the implications of policy escalation, whether it be public or discreet is a cause for concern since offensive operations can be concealed and denied with relative impunity. JTRIG’s playbook of propaganda ploys runs the risk of priming states into dangerous and irrational acts, which causes more damage in cyberspace, perhaps more than previously anticipated by GCHQ.

Moreover, Warner’s fear of another power emulating the playbook of dirty tricks takes the reader back to the original Snowden leaks on JTRIG. Considering the fact that the world is aware of JTRIG’s playbook of dirty tricks which included various measures to sway perception in foreign countries, the threshold of what states are willing to engage in is raised as a direct or indirect response of OIS within the cyber and the physical world. Each time a nation is caught engaging in such activity, others will be watching from a

distance, learning and studying *how it is done* in case an opportunity arises to wield propaganda and surveillance measures. Nations such as Russia and Iran that have inevitably observed the JTRIG Snowden leaks and have physical confirmation that global powers such as the UK are willing to deploy a raft of dirty tricks in cyberspace.

Due to this knowledge, Realist principles would indicate that other states are likely to replicate the capacity of a perceived aggressor, i.e. the JTRIG (see chapter 1). Unfortunately for the US, the 2016 election was an ample opportunity for a foreign power to test JTRIG's playbook of dirty tricks. Although GCHQ has very little to do with the discourse on the US 2016 elections, the OIS displayed by Senator Warner is the ripple effect of one nation attempting to mitigate its own OIS in various regions of the world. Without a DGC to compel intelligence services worldwide to abandon Realist overtures in the form of cyber dirty tricks witnessed in the US 2016 elections, anarchy in cyberspace will prompt an increase of OIS.

Moreover, from a different angle, perhaps American's such as Senator Warner have displayed signs of OIS because of their ontological makeup, which is predicated on power or the Realist projection of strength. The presence of multiple equals or near equals in power in a world that was briefly dominated by one superpower for the past decade is a sudden shift which has disrupted Senator Warner's sense of America's self in a Realist competitive cyber environment. This issue boils down to an example of Realism put forward in Chapter 17 of Thucydides book *The Peloponnesian War*:

*For ourselves, we shall not trouble you with specious pretences—either of how we have a right to our empire because we overthrew the Mede, or are now attacking you because of wrong that you have done us—and make a long speech which would not be believed; and in return we hope that you, instead of thinking to influence us by saying that you did not join the Lacedaemonians, although their colonists, or that you have done us no wrong, will aim at what is feasible, holding in view the real sentiments of us both; since you know as well as we do that right, as the world goes, is only in question between equals in power, while the strong do what they can and the weak suffer what they must (Thucydides, 2013).*

On an implicit level, Senator Warner understands this principle and fears that other cyber powers will engage in self-help in order to make sure that the weak suffer what they must (Thucydides, 2013). Considering that Senator Warner already perceives America as being in a place of weakness due to President Trump's unwillingness to confront Russia, perhaps Senator Warner is afraid that Russia, will continue to do what it can and America will suffer what it must. Moreover, America's dominance in the field of propaganda and surveillance which was highlighted in Chapter 3 is predicated on its habitual tendency to resort to engaging the international arena with an offensive Realist approach that aimed to bring about US dominance and ideological OS in Latin America. Very little concern was given to the weak.

Paradoxically, Senator Warner's OIS is predicated on America's OS. That is to say, America's position in the world is based on its ability and willingness to intervene in other nations affairs without much concern for collateral damage. Senator Warner's fear is based on what America became some time ago, which is a powerful rogue state that will surreptitiously intervene in the affairs of foreign nations it (America) disagrees with. The anarchical offensive Realist environment that enabled nations such as the US to violate domestic laws of other states as a means of gaining intelligence and sowing propaganda now appears to have worked in favour of other cyber powers. Fearful of a balance of power and capabilities, Senator Warner is imbued with OIS.

The knowledge that powerful adversaries such as Russia have been successful at warping perception of US citizens has clearly reduced the level of certainty that America can repel another attempt in future elections. Senator Warner's sense of OIS is pegged to the uncertainty of not being able to control the digital information space, which is becoming more and more populated with commentators and malicious actors. The more that hostile states endeavour to replicate JTRIG's playbook, the more fragmented Senator Warner's sense of OS will become particularly considering that the US President is adamant that Putin is innocent (Trump, 2018, cited in BBC, 2018[b]).

Perhaps Senator Warner should direct his concerns with GCHQ as it was the Snowden leaks that revealed to the world JTRIG's playbook which was dated back to 2011, several years before the 2016 US presidential election. At this stage of the discussion, the dream



of implementing a DGC seems slim since nations such as Russia wish to take advantage of JTRIG's playbook of dirty tricks.

Theoretically, Kant's cosmopolitanism would undoubtedly help to alleviate Senator Warner's experience of OIS, if nations could unite in cyberspace to root out international dirty tricks campaigns. Without an objective international arbiter to keep all countries in line with the rule of law, propaganda will be a prominent feature of elections and day to day life. Unfortunately for Senator Warner, his fears concerning other nations replicating Russia's covert propaganda activity will continue to haunt him provided that cyberspace remains an anarchic domain that is devoid of cyber stability and subject to cavalier international propaganda and surveillance campaigns.

---

## 5.4 Senator Elizabeth Warren

---

In the case of Senator Warren, OIS was the most prominent out of the three Democratic Senators. States can establish a sense of OS in rehearsing dangerous relationships that could bring about conflict, so long as they are clear about who the enemy is and have prepared scripts for why it is historically and contemporarily relevant to maintain hostilities. As the adage goes, *better the devil you know than the devil you do not know*. The element of the unknown makes it difficult for state figures to construct a consistent narrative which enables a nation and its inhabitants to direct resources to confront this looming enemy.

A testament to this claim is the fact that the intensity of Senator Warren's narrative fluctuated, from asserting possibilities of Russian interference to a definitive depiction of Russian President Vladimir Putin, in order to restore continuity in America's hostile Russian script. During an interview with the Associated Press, Senator Warren marked her boundary of political safety by using the word, *if*, in reference to Russia's dirty tricks campaign, which did not suffice in relation to America's ontologically hostile script with Russia. This changed immediately to paint a clearer picture of the problem at hand. Accordingly, Senator Warren stated that:

*How concerned am I on a scale of 1 to 100? I'm concerned 100. If a foreign power of any kind is trying to interfere in our basic democratic functioning, that's, that's all, all alert... and its someone like Vladimir Putin who is clearly messing around the rest of the world to try to advance Russia's interest, then it just doubles my concern* (Warren, 2016, cited in Associated Press, 2016).

What is on display in this example is the ontological need to pivot back to a safe place of political certainty and historical animosity concerning Russia's actions on the international stage. Senator Warren did not feel comfortable inundated with possibilities of who was responsible for the US 2016 election controversy. Therefore, it was necessary to juxtapose this with a definitive description of the *other*. The word, 'clearly', negates the previous rhetorical mistake made in using the word *if* (Associated Press, 2016). Cognisant of the fact that it is difficult to make definitive attributions in the cyber world, Senator Warren's juxtaposition from uncertainty to certainty demonstrates that in times of OIS it is necessary to pivot back rhetorically and ontologically to a script which serves to ease fears of the unknown in intelligence matters.

Moreover, the significant degree of concern displayed in Senator Warren's remarks is symmetrical with Ekatherina Zhukova conception of OS (2016). According to Zhukova, '[o]ntological insecurity is thus understood as a feeling of disorder, discontinuity, stress, anxiety and negative emotions' surrounding constructions of history and how state leaders act upon such constructions (2016, p.335). Judging from this definition, in conjunction with Senator Warren's statement, her concern about the US is predicated on the order of the outside world. That is, Putin messing around the rest of the world places America in an unstable environment of disorder, which in turn, reifies Senator Warren's first admission of concern (Associated Press, 2016). In other words, Senator Warren's OIS is based upon an unstable anarchical international environment that America operates within. The perceived difficulty in manoeuvring through the international arena complicates how the US perceives its sovereignty and ability to host democratic elections without alloyed Russian participants.

The work of Subotić, on the other hand, has demonstrated that narratives can be 'activated and deactivated to provide a cognitive bridge between physical insecurity ... and continuing biographical continuity of the state' (Subotić, 2016, p.617). In order to adapt

and adjust to situations that require compromise ‘policy change proposed has to fit within the overall narrative schematic template to make sense to the public, it can be crafted in a way that emphasises some parts of the story and conveniently forgets others’ (Subotić, 2016, p.611).

Conversely, at the 2018 Helsinki summit, President Trump rebuked the USIC assessment of Russian interference in the US 2016 election and defended Russia’s involvement in stating that "President Putin says it's not Russia. I don't see any reason why it would be" (Trump, 2018 cited in BBC, 2018[b]). When President Trump attempted to activate a new script that is antithetical to the USIC view on Russian interference, Senator Warren ceased to equivocate by accentuating the US-Russia hostile script. During a post-2018 Helsinki Summit interview, Senator Warren indicated that:

*That’s the part that’s most deeply disturbing. Here we are with Russian agents who have been indicted for hacking into the American electoral system. Can we just say this another way? For a cyber-attack on the United States of America. And an administration that not only is not doing enough to defend and to push back, is basically covering its ears saying ‘la la la I can’t hear you it didn’t happen’ because this is an administration focused on only one thing, not the protection of the United States the protection of Donald Trump personally (Bloomberg Politics, 2018).*

The discursive aim behind Senator Warren’s statement is twofold. Firstly Senator Warren construed Russia as the past and present threat to the US in order to pull America back to the national ontological script. Secondly, Senator Warren intended to suggest that the current US administration is willing to make an unequal exchange of protecting President Trump at the cost of damaging the nation. To begin with, Senator Warren’s response is clear and direct with who is to blame for electoral interference.

At no stage is there any attempt to deactivate or completely shift any narrative or historical biography of US – Russian relations. This is a direct response to President Trump’s actions that sent shockwaves through America’s OS by appearing to defend a decades-long enemy, who is believed by the USIC to have purposefully attempted to interfere in the 2016 presidential election.

Pivoting back to President Roosevelt, announcing the long list of issues that faced America's armed forces in the Pacific while maintaining that the US will obliterate any future attempts by an adversary to harm America, provided a sense of OS and agency to operate within an anarchic terrain. In President Roosevelt's words '[i] believe that I interpret the will of the Congress and of the people when I assert that we will not only defend ourselves to the uttermost but will make it very certain that this form of treachery shall never again endanger us' (Library of Congress, 1941). Considering how capricious and anarchic the modern cyber environment has become, Senator Warren experiences OIS because President Trump has not taken bold steps to curtail fears of future attacks as other previous wartime presidents have done. America is, therefore, unable to pivot to a place of safety before launching forward with confidence into an anarchic environment. To some extent, narratives from President Roosevelt and Bush offer examples of attempts to build a sense of OS.

However, it is necessary to juxtapose Senator Warren's response with those of Republican Senators in order to understand how political figures construe OS and respond to attempts by opposing factions (Democrats) in order to make OIS a partisan issue. Firstly, Post Helsinki, Republicans, as well as Democrats condemned President Trump's denial of Russian involvement in the US 2016 elections (Bloomberg Politics, 2018; C-Span, 2018). Republican Senator John Kennedy took an interesting approach which balanced his concerns about President Trump's resilience concerning Vladimir Putin but also rationalised the approach that President Trump took. During an interview with CNN, Senator Kennedy attempted to diffuse OIS concerns about President Trump's 'uncertain' approach by suggesting an element of unity among senators who have warned Russia about its actions while characterising President Trump's approach to feeding a dangerous animal:

*He was very uncertain, very tentative. He was clearly off his game... I told my better half [wife] Becky I said Becky 'I'm not sure what the president said'. Now he's cleared it up and regardless of what anybody says I stand by what I said about Mr Putin; dealing with him is like hand-feeding a shark he even has eyes like a shark no disrespect. Forget what he says watch what he does. If he meddles*

*in our election this fall, and I've told his colleagues this when I was in Russia as did the other Senators if he messes in our elections this fall I believe Congress will double down with sanctions maybe triple down (CNN, 2018).*

From this perspective, Senator Kennedy is trying to present America's safety as being in peril while simultaneously explaining that the logical thing to do was to interact gently with the shark (Russia) in order to prevent the US from being devoured. Additionally, Senator Kennedy's emphasis on the potential for the US Congress to triple down on sanctions on Russia for meddling in US affairs was mentioned after highlighting a collection of US Senators who acted in unity to confront Russia. This would suggest that Republicans are taking the matter of Russian interference seriously, which would indicate that America has not lost its agency to act domestically and within the international arena as a result of experiencing OIS.

In addition, Senator Kennedy is not the only Republican who has publicly highlighted the potential for tough sanctions to be placed on Russia for its election interference. Republican House Speaker Paul Ryan acknowledged Russia's 2016 election interference but spoke candidly about America's response which repudiates Senator Warren's partisan claims. In the aftermath of the 2018 Helsinki summit, Speaker Ryan made the following response concerning President Trump's denial of Russian interference in the US 2016 election:

*Let's be very clear just so everybody knows Russia did meddle with our elections. Not only did Russia meddle in our elections they're doing it around the world. They did it to France they did it to Moldova they're doing it to the Baltics. Russia is trying to undermine democracy itself to delegitimise democracy... the point we are making here is we know they interfered with our elections and we have passed sanctions on Russia to hold them accountable ... what we intend to do is to make sure they don't get away with it again and also to help our allies. To help those democracies those new and older democracies in the world who are going to be facing... this Russian aggression again we need to make sure we equip them with the tools they need to stop this from happening (C-Span, 2018).*

Speaker Ryan has attempted to forge a sense of international duty and unity among allies in response to Russia's activities which seems to contradict Senator Swalwell's concerns about a virus that is impeding America. Moreover, Speaker Ryan's words also suggest that Republicans are taking the issue of Russia and election interference seriously. Essentially, America is helping to provide the antidote to other nations to reassure allies states before elections, which again contradicts Senator Swalwell's previous comparison and also undermines Senator Warren's aforementioned partisan claims. To an extent, Speaker Ryan is attempting to shape international unity as a means of forging US OS within a multilateral framework. Evidently, OIS is present amidst the narratives of Republican and Democrats; however, Democratic Senators were far more zealous in their attempts to plunge America's OIS to trigger what they would deem to be a legitimate response that is tantamount with how the US has previously dealt with adversaries.

Moreover, the issue of attribution when grappling with cybersecurity and intelligence issues within a quasi-blameless environment leaves the USG and its citizens vulnerable and suspicious of who might be attacking them. In order to reinforce some sense of OIS, members of the USG such as Senator Warren have presented a character or entity to oppose as a means of eliminating the anxiety of facing an unknown enemy. Moreover, Senator Warren, much like Senator Swalwell also displayed signs of OIS on the basis of being imbued or consumed with risk-based projections of future realities:

*I'm hearing from both Democratic and Republican Senators who are saying they're very concerned and believe we need a full and thorough investigation. Sure right now, The Russians may have helped the Republicans, but I think everyone understands next time around it could be different. We don't want the Russians determining the outcome of our elections (Associated Press, 2016).*

At present, there is no unequivocal evidence to suggest that Russia was behind the 2016 attack nor to indicate that they will do so again in future elections. However, the very nature of propaganda and surveillance campaigns which are designed to be difficult to trace back to a state (s), pushes observers into a calculative state, continually weighing up risks and possibilities based on incomplete pictures of the past present and future. Consequently, Senator Warren is gripped with OIS as a result of uncertainty hanging over the US concerning the potential risk of another propaganda and surveillance campaign.

Much like the response of Senator Warner, Senator Warren's response is equally fearful of the same playbook being used in the near future to disrupt the US electoral process.

---

## 5.5 Conclusion

---

A consistent theme that all senators explored was a future attack and the need to be prepared. Often, this theme was predicated on sowing together a physical and ontological sense of unity. Readers can infer from the examples provided that OIS and concerns about risk often exacerbate Realist narratives of state competition. This was a prominent theme in Senator Warner's speech that focused on other adversaries that will use the *playbook* against the US in the future. Interestingly, from the examples provided, very little was spoken about reducing state tensions by mediating with Russia. This pulls the conversation back into the Realist paradigm of state competition, which fuels confrontations. Only this time, the focus is on addressing confrontation in the cyber world. However, it is essential to note that US President Obama spoke of international norms to avoid a cyber-arms race (Obama White House, 2016[a]). Conversely, as alluded to in Chapter 3 and 4, mitigating intelligence incursions with international partners will be challenging to implement due to the nature of covert activity in cyberspace by states such as the US that attempt to degrade the security (cyber) of other countries (see chapter 3). Alas, governments seem to be caught in a constant struggle for security, whether it be physical, cyber or ontological. The advent of the information age has placed a significant strain on governments and its citizens to manage their sense of OS without lunging into provocative narratives towards regional or international adversaries.

Overall, the point to be made is that the original leaks by Snowden have contributed to the knowledge that states genuinely attempt to interfere online with the perceptions of other nations. Although it is hard to prove a causal relationship between the Snowden leaks concerning JTRIG's international propaganda ambitions and Russia's alleged interference during the US 2016 elections, this case study suggests that there is a need to develop a capacity to use dirty tricks in order to keep up with adversaries. Considering that propaganda and surveillance campaigns are covert, the possibility of the Russians returning only serves to increase OIS. In an attempt to mitigate anxiety at state-level politicians are quick to maintain strong narratives about their adversaries (Russia) as a

means of stabilising the imagination and direction of a potential response. Deviation from the script would have left the US lost amidst the litany of possibilities. Therefore, in times of crisis concerning propaganda and surveillance, future depictions of danger are necessary to help stimulate the resources of a state to protect itself physically and ontologically.

Without an unshakable international arbiter or a DGC that can deter nations into relinquishing dirty tricks campaigns, countries will continue to engage in the Realist concept of 'self-help' to deal with issues in cyberspace (Evans and Newnham, 1998, p.465). Self-help can manifest as propaganda and surveillance endeavours in cyberspace in which Russia and GCHQ have demonstrated. Havercroft and Prichard have associated anarchy and Realism with conservative retrograde politics (2017, p.253); however, the lens of Realism, particularly offensive Realism, is the prevailing theory that reflects the current environment within cyberspace. Cognisant of the fact that the IRD conducted multiple propaganda campaigns in Nigeria and Latin America, it is of no surprise that British intelligence services have continued a policy of covertly shaping international affairs. The continuum from WW1 propaganda to the IRD to JTRIG demonstrates that the world indeed is subject to an anarchic environment described by Waltz, in which nations such as Britain forge dirty tricks to mitigate OIS and execute foreign policy objectives (Waltz, 1986, p.98-108).

This does not mean that Liberalism in the form of the UN or other non-state organisations such as FireEye or Kaspersky that seek to establish cyber stability have failed to impact cyber stability and IR. Instead, I suggest that the relentless strife between states and non-state groups in cyberspace has a greater gravitational force than Liberalism. Cyber stability is subject to the direction and whims of powerful rogue states and non-state groups who seek to disrupt the international rules-based system as a means of accumulating power and the ability to warp perception in cyberspace.



---

## Chapter 6, Case Study 2: The Democratic Proselytisation of Non-State Terror and the FBI's Sham Universe

---

So far, a litany of evidence has been presented to demonstrate that the intelligence services of various nations use the Internet to sow deceit and construe favourable narratives (see chapter 1 and 3). Chapter 3 and 4 has shone a light on how integral propaganda and surveillance measures are for democratic states. Furthermore, the debate within Chapter 4's literature review has indicated that propaganda is a crude but paradoxically vital component of Western democracies. Keeping *the barbarians at the gate* while preventing democracy from mimicking and mastering vices that are allegedly better suited to authoritarian regimes is a near-impossible task. Within an anarchic environment comprised of multiple threats to many countries, emulating the most amoral acts in order to keep the barbarians out of bounds has become common logic for the so-called democratic leader of the free world, the USA.

Political figures from the Republican and Democratic Party in the US, often spend time pontificating against the systemic vices of Islamic extremists and their proxies that support terrorism in cyberspace. In the words of Condoleezza Rice, President George W Bush's former National Security Advisor, '[t]rue victory will come not merely when the terrorists are defeated by force, but when the ideology of death and hatred is overcome by the appeal of life and hope, and when lies are replaced by truth' (George W Bush White House Archives, 2004). Similarly, in 2016, President Obama stated that 'we have to uphold the civil liberties that define us. Terrorists want us to turn on one another...we have to make sure changes in how we address terrorists are not abused' (Obama White House, 2016[b]).

In a dramatic U-turn on American democratic values, the FBI has conceded to the fact that they engaged in surreptitious activity online which included setting up a fake terrorist website to lure people in and communicate with them via fake aliases ('United States Of America v. Abdella Ahmad Tounisi, 2013, p.19). Those interested would be convinced by the FBI to fly to Syria and fight on behalf of Jabhat al-Nusrah, only to be stopped at a US airport by undercover government agents ('United States Of America v. Abdella Ahmad Tounisi', 2013, p.19-20).

Coincidentally, this activity resembles the online propaganda and misinformation ambitions of JTRIG (see chapter 1 and 3). Ironically, the FBI has described domestic terrorism as being carried out ‘by individuals and/or groups inspired by or associated with primarily U.S.-based movements that espouse extremist ideologies of a political, religious, social, racial, or environmental nature’ (FBI, n.d.[c]). However, this case study demonstrates that the FBI knowingly created a propaganda website for the world to see and fall prey to. The paradox created by the FBI has encouraged me to refer to such behaviour as the democratic proselytisation of terrorism. Proselytising terrorism seems to run contrary to Western democratic ideals, yet the FBI decided to push propaganda on the Internet in the name of protecting its democracy from potential terrorists.

In this chapter, I will present and analyse the case of the FBI’s online sting operation in what appears to be a well-laid trap to inculcate an American citizen with propaganda and lies. This will be complemented with discussion on whether or not the FBI’s tactics are synonymous with or a form of entrapment and the extent (if at all) to which Tounisi’s human rights were violated. Evidence will be taken from the affidavits presented in court by the FBI’s SA. Moreover, the purpose of this chapter is to provide scrutiny towards the FBI’s propagandistic and deceitful technique of establishing online aliases which sought to encourage discussion and incite the desire to commit terrorism. In doing so, this chapter will be helping to plug the gap in knowledge concerning modern propaganda and surveillance activities of Western intelligence services.

Additionally, this chapter aims to assess one of the objectives of this thesis, which is to demonstrate that attempts to mitigate OIS in the cyber world can end up producing more state anxiety or concerns for citizens. It is also worth noting that this chapter will assess JTRIG’s playbook that was an issue for Senator Warner in Chapter 5. Before engaging in the case of Tounisi, I will highlight the FBI’s Net Talon National Initiative (NTNI). The NTNI provides online FBI agents with the freedom to create a propagandised sham universe which helped to engineer the democratic proselytisation of terrorism.

---

## 6.1 Net Talon National Initiative

---

In the 21<sup>st</sup> century, the FBI has adapted its propaganda and surveillance methods to warp perception online and track targets. The NTNI is an ‘online, undercover, national initiative constructed to strategically focus operations (using OCEs UCEs and CHSs) targeting terrorists use of the Internet’ (FBI, 2015, p.20). As maintained by the FBI:

*The perceived anonymity, security, and efficiency of online communications have attracted the attention of terrorist, their facilitators and their sympathizers. The result has been an explosive growth of terrorist using the Internet for communications, propaganda dissemination, fundraising, recruitment, operational planning, training and radicalization (FBI, 2015, p.50).*

As a result of developments within cyberspace, the FBI has chosen to alter its methods of investigations to keep pace with impending threats. The FBI’s NTNI mandate is to ‘detect, penetrate, disrupt, and dismantle online terrorist networks’ that have begun making use of the sizable reach that cyberspace offers (FBI, 2015, p.50). Also, the FBI’s NTNI program endeavoured to:

*Know, monitor, and target any adversary’s online domain... To develop and manage online resources to maximize HUMINT penetration into online terrorist networks...the NTNI allows visibility into online activities of all OCEs, UCEs and CHSs targeting IT subjects and provides a program to ensure they are tasked according to their skill sets and workloads (FBI, 2015, p.50).*

For the sake of clarity, an OCE is an FBI Online Covert Employee (OCE), a CHS is referred to as a Confidential Human Source (CHS) and UCE is an Undercover Employee. To maximise the reach and effectiveness of online activity, the FBI deemed it desirable to share intelligence and conduct joint operations with the USIC and ‘foreign intelligence and law enforcement partners’ (2015, p.17). On the authority of the FBI ‘[t]he NTNI will support these joint operation and has the capability to utilize all the resources and tools available to the FBI, USIC and international partners’ (2015, p.51). As will be discussed towards the end of this chapter, the extent to which international partners and the UK helped to maintain this sham universe is an unanswered question that makes this

conundrum all the more problematic. In terms of guidance and direction for engaging targets, undercover operatives were informed that ‘OCE or a UCE may engage in unlimited communication with associates of that predicated subject for the purpose of gaining additional intelligence or evidence on the predicated subject’ (FBI, 2015, p.67).

However, an inevitable point of semantic controversy is how to interpret or even decide when intelligence gathering and communications turns into something more sinister such as entrapment. Agents were informed by the FBI that if they develop ‘sufficient derogatory information regarding the associate...the purpose of the communications changes to gathering intelligence’ (2015, p.67). As will be discussed further down in this chapter, extricating the difference between gathering intelligence and directly making suggestions to an unwitting Internet user that fighting for a terrorist group in Syria is a noble Islamic idea, is revealing of multiple selves that uphold democratic and amoral ideals.

Moreover, what is more frightening from this policy is the fact that operatives are given the freedom to engage in an unlimited amount of communications with those who are not under investigation. According to the FBI:

*For the purpose of establishing bona fides and credibility, OCEs and UCEs may make postings and communicate with individuals who are neither the subjects nor the associates of subjects of assessments or predicated investigations. There is no limitation with respect to the amount of communication an OCE or a UCE may initiate in this regard (2015, p.67).*

Therefore, if a target is located who is vulnerable and susceptible to temptation, the FBI is free to inculcate this individual with nefarious suggestions until he or she is ready to commit an act of terror.

---

## 6.2 The OCE's and Entrapment

---

An additional contentious area of discussion is whether or not the use of undercover sting operations by FBI and other law enforcement agencies should be considered as entrapment. A typical sting operation consists of a secret agent or informant that encourages a criminal or innocent individual to take part in some form of illegal activity. The logic of sting operations is to test and capture people who are willing to commit crimes. Cyberspace provides law enforcement and intelligence services with a relatively new medium to construct pervasive sting operations. However, it must be noted that this relatively new opportunity also comes with the risk of 'overzealous law enforcement in cyberspace' (Hanson, 1996, p.535).

Within US law enforcement agencies 'sting operations are premised on the idea that individuals who would participate in schemes initiated by FBI informants might otherwise have been approached by an actual terrorist recruiter' (The Center of Law and Security, 2011, p.7). Cyberspace provides operatives with the ability to assume false identities, which may indicate the 'probable increase in undercover sting operations' (Hanson, 1996, p.536). Undercover sting operations from US law enforcement agencies have had a significant rise since 9/11. In the opinion of the Center of Law and Security 'Since 9-11, 41% of terrorism cases have involved an informant' (2011, p.28).

Moreover, sting operations predominantly consist of law enforcement operatives surreptitiously creating and facilitating the conditions and the means of the offence in question (Hay, 2005, p.3). The steep rise in sting operations seems to correlate with the 300 prosecutions between the years 2001 to 2011 that 'resulted in indictments related to jihadist terror or national security charges' (The Center of Law and Security, 2011, p.4). Nonetheless, the question of entrapment continues to surround the FBI. Sting operations that foster the encouragement of criminal activity by law enforcement operatives perhaps 'should be allowed only when law enforcement officials can demonstrate reasonable suspicion that the suspect is involved in ongoing criminal activity' (Whelan, 1985, p.1197).

Determining the extent to which law enforcement can demonstrate suspicion is controversial and subject to scrutiny (Tawil, 2000, p. 2376). Conversely, entrapment defence in the US ‘potentially applies whenever a defendant commits an offense facilitated by undercover government agents’ (McAdams, 2007, p.1796). Although entrapment is interpreted differently around the world, this case study is based on America’s interpretation. Therefore, throughout this chapter, entrapment will be explored with an American understanding and legal standards. To begin with, it is vital to define the term entrapment.

According to the US Attorney General's guidelines on FBI undercover operations in the early ‘[e]ntrapment occurs when the Government implants in the mind of a person who is not otherwise disposed to commit the offense the disposition to commit the offense and then induces the commission of that offense in order to prosecute’ (US Department of Justice Archives, 2017). Furthermore, the Department of Justice has stated that ‘[a] valid entrapment defense has two related elements: (1) government inducement of the crime, and (2) the defendant's lack of predisposition to engage in the criminal conduct... Of the two elements, predisposition is by far the more important’ (US Department of Justice, n.d.[a]).

This definition is predicated on previous infamous court cases in which successful entrapment defences were held. For example, in the case of *Sorrells v United States*, a government agent had become acquainted with the defendant (Sorrells) and asked him three times for some liquor (Hanson, 1996, p.537). After the third request, Sorrells provided half a gallon of liquor (Hanson, 1996, p.537). The defendant was indicted for possessing and selling half a gallon whisky (Cornell Law School, n.d.[a]). During *Sorrells v United States* in 1932, Chief Justice Hughes delivered his opinion stating that:

*It is clear that the evidence was sufficient to warrant a finding that the act for which defendant was prosecuted was instigated by the prohibition agent, that it was the creature of his purpose, that defendant had no previous disposition to commit it but was an industrious, law abiding citizen, and that the agent lured defendant, otherwise innocent, to its commission by repeated and persistent solicitation in which he succeeded by taking advantage of the sentiment aroused by reminiscence (Library of Congress, 1932, p.7).*

Chief Justice Hughes was concerned about the individual who first concocted or suggested the plan to engage in criminal activity. This is not to suggest that the crime itself was not an issue. Chief Justice Hughes recognised the criminal activity of Sorrells but maintained that Sorrells ‘has committed the crime in question, but, by supposition, only because of instigation and inducement by a government officer’ (Library of Congress, 1932, p.24). The instigation of a crime is thus necessary to contemplate when assessing an entrapment defence.

Furthermore, to put the Department of Justice’s aforementioned description of entrapment into context, during the case of *Jacobson vs United States*, the defendant ordered child pornography after: “[h]e had already been the target of 26 months of repeated mailings and communications from Government agents and fictitious organizations” concerning the purchase of child pornography (US Department of Justice, n.d.[b]).

However, in the past, the defendant had obtained a copy of an explicit magazine depicting teenage and pre-teenage nude images from a book store. Law enforcement agents identified the defendant’s name on a mailing list and began conjuring a plan to induce Jacobson to order child pornography. In the view of the supreme court, the government had failed to unequivocally prove that Jacobson's predisposition "was independent and not the product of the attention that the [g]overnment had directed at [him][.]" (US Department of Justice, n.d.[b]).

Jacobson claimed entrapment against the USG because undercover operatives were repeatedly targeting him for a lengthy period. Although ordering child pornography is a crime and a deplorable thing to do, US law enforcement was heavily scrutinised because it became difficult to prove that Jacobson had an unequivocal disposition to ordering child pornography before undercover operatives decided to initiate a lengthy campaign of inducement. On the contrary, even if inducements were persistent, a claim of entrapment under US law may not be held if the defendant was already predisposed to committing a crime. In the case of *Jacobson v. United States*, it was cited that:

*[I]f the defendant before contact with law enforcement officers or their agents did have an intent or disposition to commit the crime charged, then he was not*

*entrapped even though law-enforcement officers or their agents provided a favourable opportunity to commit the crime or made committing the crime easier or even participated in acts essential to the crime* (Justice White, 1992 cited in Justia, 2018).

Similarly in the conclusive ruling of *Sherman v. United States*, it was held that entrapment was established by law enforcement operatives who used an informant to encourage a recovering drug addict to supply drugs to the informant (Chief Justice Warren, 1958, cited in Justia, 2019[b]). Moreover, the understanding of entrapment defence has expanded to include an additional requirement. During the court case of *United States v Hollingsworth*, Chief judge Posner having interpreted the ruling in *Jacobson v United States* added scrutiny to the concept of predisposition. Chief Judge Posner asserted that the person in question must also display readiness, to commit a crime, because a person can have dreams of being a criminal but lack the means to do so (Chief Judge Posner, 1993, cited in Casetext, 2019).

The readiness element would suggest that the defendant has the knowledge and capacity to carry out a crime (Tawil, 2000, p. 2376). David Tawil has provided clarity on the concept of readiness (Tawil, 2000, p. 2376). If a random individual, Joe, wants to launder money but has no experience of doing so and also lacks the connections, the court would find entrapment in the case that the government provided the essential connections and knowledge on how to launder money (Tawil, 2000, p. 2376). On the other hand, if the government could prove that Joe was aware of how to launder money and had the connections to do so before government agents contacted him, the entrapment defence would be rejected (Tawil, 2000, p. 2376).

Throughout this chapter, references will be made back to the complexities of interpreting entrapment and intelligence work. This decision is vital as case 2 study revolves around a propaganda website as the initial point of contact between the FBI and people interested in terrorism that have not yet committed an act of terrorism. The value of understanding entrapment is integral to this chapter. If it is proved that the FBI's activities are synonymous with entrapment, serious moral questions will be raised.



---

## 6.3 Abdella Tounisi

---

In the first case of democratic proselytisation of terror, Tounisi, an eighteen-year-old US citizen from Illinois was a victim of online propaganda and deceit ('United States Of America v. Abdella Ahmad Tounisi', 2013, p.3). At the end of March in 2013, Tounisi made contact with an individual 'whom he believed to be a recruiter for Jabhat al-Nusrah, but who in fact was an FBI online undercover employee' ("the OCE") ('United States Of America v. Abdella Ahmad Tounisi', 2013, p.7).

The beginning of the FBI's affidavit comprises of the following pretext for democratic incitement of terror: 'Tounisi and the OCE exchanged several emails, during which Tounisi told the OCE that he planned to get into Syria by travelling to Istanbul, Turkey... Tounisi also expressed to the OCE a willingness to die for the cause' ('United States Of America v. Abdella Ahmad Tounisi', 2013, p.7). It is clear from an early point that Tounisi had an interest and a predisposition to terrorist ideation. However, as will be discussed later, it is immoral to knowingly develop this interest instead of helping Tounisi to begin a de-radicalisation program. Additionally, the SA's comments within the affidavit revealed the FBI's propaganda endeavours. According to the SA:

*During the investigation, the FBI published a webpage that purported to recruit individuals to travel to Syria and join Jabhat al-Nusrah. In particular, the top of the webpage stated, "A call for jihad in Syria," and depicted a photograph of an armed fighter. The website also included a purported Jabhat al-Nusrah training video that depicted individuals wearing masks and fatigues, and engaging in training, such as running with firearms. The website stated, among other things, "come and join your lion brothers of Jabhat al-Nusrah who are fighting under the true banner of Islam, come and join your brothers, the heroes of Jabhat al-Nusrah* ('United States Of America v. Abdella Ahmad Tounisi, 2013, p.19).

At this stage, readers can observe the deliberate attempt made by the FBI to create an environment in which people would hopefully fall prey to the allure of the websites propaganda. In relation to the FBI's fake terrorist website, the invitation to join Jabhat Al-Nusrah demonstrates the desire to mobilise action on the part of those who visited the

website. More so, the direct invitation to ‘join your lion brothers of Jabhat al-Nusrah’ in conjunction with the religious sentiment, e.g. ‘the true banner of Islam’ are further examples which leaves little doubt that this website was set up to attract people while exonerating terrorist groups (‘United States Of America v. Abdella Ahmad Tounisi’, 2013, p.19).

The most important point to make at this early stage is that the FBI’s website is unlikely to make curious people turn away from Jihad. Instead, it spurs terrorist ideation. In a democracy, this activity may be deemed as something that is better suited to an authoritarian regime. Nonetheless, stimulating terrorist ideation also increases the potency of the sham universe. Avenues were provided to turn curiosity into a hardened desire of becoming a fighter in Syria. The following admission sheds light upon the extent that the FBI was willing to aggrandise the scale of its democratic sham universe. According to the affidavit, the SA stated that:

*The website provided an email account as a point of contact, along with instructions ... We are aware of the Kuffar tricks and the behaviour of their unjust governments. We also understand the risk of direct contact. Therefore you can contact us via email so that we provide you with the required information which will help you to set off for your jihad in Syria. Before sending us an email, create a new email that you have never used before and send the email to us from a public place* (‘United States Of America v. Abdella Ahmad Tounisi’, 2013, p.19-20).

A poignant issue for the undercover agents in the above scenario is maintaining the sham universe. Seen as the FBI have done such an impressive job of creating the website in conjunction with authentic emails, the agents must maintain and increase the potency of messages communicated to keep Tounisi interested. However, keeping Tounisi interested in fighting abroad will inevitably involve the FBI glorifying terrorism. Put bluntly by Omand ‘[a]ny important agent in place inside a terrorist network is, for example, likely to be involved in criminal [behaviour]—otherwise he or she is unlikely to continue being in a position to acquire the inside information being sought’ (Omand and Phythian, 2013, p.51).

If readers follow Omand's view as a given maxim of intelligence collection, it would appear that the democrat must concede to lowering the moral democratic bar that the West is fixated with, to triumph over an adversary. Moreover, it is worth pointing out that the appropriation of crucial trigger words such as 'Kuffar' acts as linguistic paraphernalia that only serves to cajole those who view non-Islamic believers (Kuffars) as being an enemy of progress that needs to be vanquished ('United States Of America v. Abdella Ahmad Tounisi', 2013, p.20). Keeping in line with propaganda theory, Lasswell highlighted the importance of sensitive words as a part of an overall strategy of manipulation. According to Lasswell:

*The strategy of propaganda, which has been phrased in cultural terms, can readily be described in the language of stimulus-response. Translated into this vocabulary, which is especially intelligible to some, the propagandist may be said to be concerned with the multiplication of those stimuli which are best calculated to evoke the desired responses, and with the nullification of those stimuli which are likely to instigate the undesired responses (Lasswell, 1927, p.630).*

From this insightful perspective, it is of no surprise that the FBI decided it was necessary to use sensitive words in an appropriate context that would likely stimulate resentment amongst those who have fallen prey to the (FBI's) website. Enticed further by the FBI's fake terrorist website, Abdullah willingly responded in the hope that a terrorist group would guide him:

*My name is Abdullah and I am planning InshaAllah to join my brothers in Syria in April. InshaAllah I'am going to buy two tickets one from Chicago to Istanbul and another from Istanbul to Gaziantep. I do not know what to do after I arrive in Gaziantep because I do not have any contact information. Can you please help me modify my plain if it needs modification and to prove the authenticity of this e-mail service. Please give me a reply soon as possible ('United States Of America v. Abdella Ahmad Tounisi', 2013, p.20).*

The FBI responded to this on the 29 of March in 2013, stating that:

*Brother, Abdullah, [w]e received your email. Our security procedures demand that we create a new email and start communicating through it. We have plans to*

*move you safely insha'Allah as you requested in your email. The below [email address] is the only way for you to communicate with us from now on and is created only for you* ('United States Of America v. Abdella Ahmad Tounisi', 2013, p.21).

Albeit Abdullah took it upon himself to email the account left on the fake website, the FBI persisted with the guidelines highlighted in the NTNI which states that undercover operatives do not have a limitation concerning communicating with targets (FBI, 2015, p.67). With this in mind, secret agents have the license to continuously tempt people that have already fallen prey to extremist ideology, and potentially or inadvertently push them deeper into the imaginative cesspool of terrorist ideology.

Most importantly, the Bureau is guilty of dangling more jihadi carrots in front of Tounisi by emphasising the extent to which they can get him into Syria. From a psychological perspective, the concept of de-individuation and disinhibition played an integral role in helping to asphyxiate Tounisi's ability to stay in touch with reality (Festinger, Pepitone, and Newcomb, 1952, p.382; Pennington, Gillen and Hill, 1999, p.308). According to Festinger, Pepitone, and Newcomb, deindividuation refers to the 'reduction of inner restraints' in group situations (1952, p.382).

Similarly, Miles Hewstone and Robin Martin described de-individuation as 'a state in which individuals are deprived of their sense of individual identity and are more likely to behave in an extreme manner, often anti-socially and violating norms' (2008 p.224). Similarly, disinhibition refers to the 'reduction in the social influences that usually restrain people from anti-social behaviour' which would have eased Tounisi's transition into the sham universe (Pennington, Gillen and Hill 1999, p.308). In physical crowd-like settings, people are more susceptible to suggestion by a social orchestrator, which in the case of Tounisi was the FBI. This may appear to be contradictory with the FBI and Tounisi's case considering that it was one on one communication in cyberspace, but the work of Le Bon, which was the antecedent to Festinger, Pepitone, and Newcomb's concept of de-individuation suggests otherwise. According to Le Bon:

*The disappearance of conscious personality and the turning of feelings and thoughts in a definite direction, which are the primary characteristics of a crowd*

*about to become organized, do not always involve the simultaneous presence of a number of individuals on one spot. Thousands of isolated individuals may acquire at certain moments, and under the influence of certain violent emotions... an entire nation, though there may be no visible agglomeration, may become a crowd under the action of certain influences (Le Bon, 2014, p.12).*

From this angle, the FBI created the appearance of a psychological crowd in which Tounisi was under the impression that he was bound to be a part of a larger group of Muslim *brothers* that had the same passion for terrorism. To a great extent Tounisi was in a:

*Special state, which much resembles the state of the fascination in which the hypnotized individual finds himself in the hands of the hypnotizer. The activity of the brain being paralyzed in the case of the hypnotized subject, the latter becomes the slave of all the unconscious activities of his spinal cord, which the hypnotizer directs at will (Le Bon, 2014, p.16).*

The consequence of being a part of a psychological crowd is that ‘[u]nder the influence of a suggestion, he will undertake the accomplishment of certain acts with irresistible impetuosity’ in the same way as one would if they were a part of a mob (Le Bon, 2014, p.16). Judging from the literature above, a case can be made that the presence of false information will mislead people into a state of mind that is vulnerable to suggestion. As a result, the individual is lost in a digital sham universe and is subject to the mercy of a propagandist which in this case is the FBI. In the case of Tounisi, suggestions that were made by the FBI served as a mechanism of genuine inquiry in conjunction with stimulating his obedience to the notion of committing Jihad in Syria. Without doubt, public revelations of the FBI’s covert activity in cyberspace will induce a sense of OIS among Internet users.

Additionally, a concern to acknowledge is the possibility that Internet users who are not terrorists may become fearful that the anonymous people they are communicating with are actually intelligence operatives. Cognisant of the fact that the ECJ ruled that keeping communications data for extended periods may lead to the feeling of continuous surveillance, maintaining an NTNI can produce similar feelings with regards to the

concern about being duped online by intelligence operatives (Court of Justice of the European Union, 2014, p.1-2) (see chapter 3). In other words, it is possible that the information diet of citizens may change to the extent that people avoid consuming information online and from governments due to the perceived spectre of covert propaganda that haunts citizens after amoral intelligence operations have been revealed to the public. At first glance, this may indirectly suggest that a change in the information diet is unhealthy and irregular.

On the contrary, the predominant concern is the lack of trust in information which can foster a deep sense of unease about engaging in essential matters that impacts the future direction of any given country. The concerns about trust of information can evolve into concerns about trusting government information, regardless of whether what is communicated has anything to do with information provided by the FBI, GCHQ or any unit.

In light of the fact that a large portion of crucial national security information is provided by intelligence services, which at times trickles its way down to citizens as a means of justifying war or hostile foreign policy measures; the paralysis in perception and faith of information can be dangerous for policymakers who seek societies approval to move forward with risky foreign policy endeavours. In 2018 Russian media outlets mocked the British Prime Minister May for her intelligence assessment which stated that it was *highly likely* that Russia was behind the poisoning of Sergei Skripal in the UK (see figure 24). Russia turned this probability into a parody by uploading a video to Twitter, stating that Russia ought to be blamed for the snow in Britain. In conjunction, Russia's state-owned RT outlet referred to the assassination attempt as a 'Novi – cock up' and later reminded people of Britain's past intelligence failures with titles stating '15 years after Iraq War, same old MPs jump on chemical weapons claims in Skripal poisoning' (see figure 25) (RT, 2018[a]; RT, 2018[b]).



Figure 24: Ministry of Foreign Affairs Russia, 2018



Figure 25: RT 2018[a]

So long as intelligence services are seen to be Orwellian and permeated with truculent endeavours, public opinion within democracies are at risk of being paralysed by cynicism and foreign influence that aggrandises the distrust for information. It is, therefore, in the best interests of intelligence services such as the FBI to balance how they carry out intelligence practices to avoid information campaigns that could greatly influence US public opinion and the efficiency of its (US) foreign policy endeavours.

Moreover, to further emphasise the FBI's willingness to lure Tounisi into criminal activity, Tounisi expressed concerns about his financial resources and how feasible it was 'to travel from Istanbul to the border of Syria' ('United States Of America v. Abdella Ahmad Tounisi', 2013, p.22). On April 2<sup>nd</sup>, the OCE continued to encourage and alleviate Tounisi's fears as opposed to solely gathering intelligence. The OCE stated that:

*We have moved brothers over here before so we know exactly what we do from there. All you have to do is tell us what date you will arrive to Istanbul and we*



*will take care of the rest and provide you with details insha'Allah... we have trust in Allah that you will fight and do your Jihad as a true mu'min ... As you know that Shahada is the ultimate desire of any Mujahid, so with that in mind, brother Abdullah, we ask if you are willing to be a shaheed if the will of... Allah comes upon you to be one? ('United States Of America v. Abdella Ahmad Tounisi', 2013, p.22).*

Encouragement and incitement is a running theme within the FBI's communication attempts. Again, the undercover agent incorporated concepts of religious duty and blind faith to create a sense of ease with regards to transportation issues. What is striking from this example is the litany of words 'mu'min...shahada... 'Mujahid...Shaheed' that is appropriated from Jihadist extremist to espouse a grand and sincere invitation to go and fight in Syria ('United States Of America v. Abdella Ahmad Tounisi', 2013, p.22). By reinforcing the concept that 'shahada is the ultimate desire of any Mujahid' the undercover agent apotheosised commitment towards terrorism before asking a question to assess Tounisi willingness to go and fight in Syria ('United States Of America v. Abdella Ahmad Tounisi', 2013, p.22).

Although it is evident in this example that the FBI has ticked a box for intelligence gathering, how the question is asked is geared towards incitement. The association with being chosen by God reifies the concept of deindividuation, in which Tounisi's sense of responsibility for committing heinous crimes is diminished, primarily since God can forgive sins and reward fighters in the afterlife. Conversely, it would be unwise to deny the fact that the excerpt concluded with a question that provided Tounisi with a choice.

To verify how vulnerable an entrapped individual is, readers would have to assess if the person at any stage resisted invitations by an undercover agent to engage in criminal activity. In the case of *United States v. Jorge Cortes*, it was highlighted that '[i]n determining whether the defendant was predisposed to commit the crime before being approached by government agents, you may consider the following...whether the defendant demonstrated reluctance to commit the offense' ('United States Of America v. Jorge Cortes', 2014, p.10). As it turned out, Tounisi was very eager to commit Jihad and as a result of this insatiable passion, condemned himself even further into the FBI's sham universe.

Pivoting back to the Department of Justice's boundaries of entrapment, one of the most important factors to consider is the person's predisposition to committing a crime (US, Department of Justice, n.d.[a]). However, if an individual is known to have committed a crime in his or her distant past or has recently engaged in criminal activity, the claim of entrapment may not suffice. In the conclusive ruling of *Sherman v. United States*, it was held that entrapment was established by law enforcement operatives who used an informant to encourage a recovering drug addict, Sherman, to supply drugs to the informant (Chief Justice Warren, 1958, cited in Justia, 2019[b]). Sherman was previously convicted in 1942 'for illegally selling narcotics; in 1946, he was convicted of illegally possessing them' (Chief Justice Warren, 1958, cited in Justia, 2019[b]).

Despite this record, Chief Justice Warren held that the view that Sherman's previous convictions 'are insufficient to prove petitioner had a readiness to sell narcotics at the time Kalchinian approached him, particularly when we must assume from the record he was trying to overcome the narcotics habit at the time' (Chief Justice Warren, 1958, cited in Justia, 2019[b]). In the event that someone has committed a crime in the US, his or her rights are not completely suspended. Prisoners for example 'do not have full constitutional rights' but are protected by the Eighth Amendment prohibition of cruel and unusual punishment (Cornell Law School, n.d[b]; The White House, n.d.).

US citizens are protected by the Constitution, which guarantees that all citizens are not subject to criminal prosecution without due process (The White House, n.d.). To be precise, the Fifth Amendment ensures that citizens are not 'subject to criminal prosecution and punishment without due process. Citizens may not be tried on the same set of facts twice, and are protected from self-incrimination (the right to remain silent)' (The White House, n.d.). From this angle, Tounisi is still a US citizen and is entitled to a basic set of human rights guaranteed to him under the US Constitution (The White House, n.d.).

Furthermore, previous criminal activity may not unequivocally warrant law enforcement inducements, particularly if the person in question has taken steps to dissociate his or her self from a life of crime (Chief Justice Warren, 1958, cited in Justia, 2019[b]). It would appear that Sherman at one stage in his life had a predisposition to criminal activity. However, when the case is placed in the necessary context which highlights the fact that

the undercover informant had met Sherman at a drug recovery clinic, the government's actions to ensnare a vulnerable addict would seem outlandish and legally unjust (Chief Justice Warren, 1958, cited in Justia, 2019[b]).

At this juncture, it is necessary to ponder the extent to which Tounisi's case can be extenuated in the same way that Chief Justice Warren has previously done for Sherman. To begin with, Tounisi has no previous conviction for terrorist offences. On the other hand, Tounisi was previously interviewed by the FBI back in 2012 due to concerns about his downward spiral into terrorist ideation ('United States Of America v. Abdella Ahmad Tounisi', 2013, p.23).

Moreover, Tounisi managed to come across the FBI's website and made the initial contact (to the FBI) under the false impression that he was speaking with a terrorist organisation. Considering the gravity of the situation, searching out for terrorist websites in order to ask for material support to go and fight a war in Syria may prove to be enough to suggest that Tounisi had a clear interest in taking part in terrorism and the war in Syria. Although Tounisi's senses were elevated and contorted to strengthen his resolve to fight in Syria as a result of the FBI's activity, claims of entrapment may not be taken seriously considering the US Department of Justice's stringent interpretation.

Moreover, the final and most controversial democratic jihadi carrot came in the form of probing by the OCE to assess the exact date Tounisi wanted to travel in order to "prepare a travel plan from Istanbul to where you will meet the brothers" who will take Tounisi to a training camp ('United States Of America v. Abdella Ahmad Tounisi', 2013, p.23). Consequently, this led to the OCE offering a free bus ticket. According to the SA "we will buy the bus ticket and send it to the new email address" ('United States Of America v. Abdella Ahmad Tounisi', 2013, p.26).

This was a decisive moment which helped to reassure Tounisi to embark on a long quest to go and fight in Syria. Offering an individual a bus ticket that has previously been inculcated with propaganda has made it clear that the FBI crossed a dangerous Rubicon and provided the necessary conditions to directly or indirectly incite terror. Sometime after this, Tounisi attempted to make the trip to Syria but was apprehended by undercover agents at the airport. Pivoting back to Chief Judge Posner interpretation of readiness, it

appears that Tounisi did not have the means or the connections to carry out his desire to engage in terrorism abroad (Chief Judge Posner, 1993, cited in Casetext, 2019; Tawil, 2000, p. 2376). This does not dilute his moral sin of wanting to fight in Syria on behalf of a terrorist organisation. Rather, it highlights the influence that the FBI had in encouraging a novice to believe he could become a hardened fighter in Syria.

At this late stage, the FBI's erroneous fable became so 'powerful that it invades every area of consciousness, leaving no faculty or motivation intact. It stimulates in the individual a feeling of exclusiveness and produces a biased attitude' (Ellul, 1973, p.11). It is undeniable that Tounisi had some element of control. However, the additional offer by the FBI to settle financial and logistical concerns coupled with previous incitement demonstrates that Tounisi was groomed to go and fight in Syria. Understandably, the nefarious connotation of the word grooming concerning criminal activity is antithetical with Western democracies.

However, this case study has demonstrated how the FBI can target vulnerable people. The concept of OIS emerges, as the amount of people targeted is unknown. Cognisant of how vast cyberspace is, to what extent can one be sure that the FBI or other intelligence services are not on the Internet warping perception in the name of democracy and security? People who become aware of how deceptive democratic intelligence services can be may become weary that people on the Internet might very well be government agents who are attempting to groom people into a supposed life of criminality. In conjunction with this point, Lasswell's description of propaganda manipulation is congruent with Tounisi's story of curiosity and deception:

*Some of those who trusted so much and hated so passionately have put their hands to the killing of man, they have mutilated others and perhaps been mutilated in return, they have encouraged others to draw the sword, and they have derided and besmirched those who refuse to rage as they did. Fooled by propaganda? If so, they writhe in the knowledge that they were the blind pawns in plans which they did not incubate, and which they neither devised nor comprehended nor approved (Lasswell, 1972, p.3).*

While Tounisi may never trust the Internet again, others who become aware of such clandestine endeavours may also feel OIS, not because they sympathise with terrorists, but because of the inability to say for sure that a domestic or foreign intelligence service is not interested in the political views of Internet users. Chapter 1 serves to highlight the endeavours of JTRIG, which revealed that its online playbook of dirty tricks is used to warp perception. As revealed in Chapter 5, modern propaganda conducted by Russian and Iranian entities has targeted the political views of American and British citizens in a secret manner which also relied on the creation of false personas.

With cyberspace slowly descending into a digital cesspool of lies sowed by intelligence services, OS or trust is at risk of diminishing. For many critics, defending a would-be terrorist appears like an extreme leftist notion that makes Western democracies open to terrorism. However, the key point to be made here is that it is highly questionable for the democratic leader of the free world to espouse noble liberal claims (see previous statements by President Obama and former National Security Advisor Condoleezza Rice) then indirectly or directly allow its intelligence services to incite terror.

Defending a potential terrorist may seem odd, but in countries such as the UK, preventing people from being lured into terrorism has become a critical area for the government's counter-terror policy. Since 2011 the Prevent Strategy and the 2018 counter-terror Contest Strategy has been implemented in Britain to spot signs of terrorism and help alleviate the issue as opposed to offering bus tickets to fight in Syria ('United States Of America v. Abdella Ahmad Tounisi', 2013, p.26; Home Office, 2015[b], p.3; Home Office, 2018, p.12).

However, the UK Prevent strategy has been marred by accusations of islamophobia with regards to feelings of surveillance of the Muslim community. Cited in the Prevent Strategy, the British government endeavours to '[p]revent people from being drawn into terrorism and ensure that they are given appropriate advice and support; and work with sectors and institutions where there are risks of radicalisation that we need to address' (Home Office, 2015[b], p.3). On the other hand, the Prevent strategy does not rule out the fact that UK courts have indicated that entrapment may be permissible.

Although Lord Nicholls of Birkenhead indicated during *Regina v. Loosely* that invasive techniques of entrapment should ‘not be applied in a random fashion, and used for wholesale ‘virtue-testing’, without good reason’ (*Regina v. Loosely*, 2001). The fact that police or a police informant is used does not affect the guilt of an entrapped individual but may mitigate the conclusive penalty (*Regina v. Loosely*, 2001). Furthermore, the UK Crown Prosecution Service have stated that ‘entrapment is not a substantive defence in English law’ (CPS, 2018).

On the other hand, it has been noted by Lord Hoffmann that ‘the court has jurisdiction in a case of entrapment to stay the prosecution on the ground that the integrity of the criminal justice system would be compromised by allowing the state to punish someone whom the state itself has caused to transgress’ (*Regina v. Loosely*, 2001). Entrapment as a process is not a phenomenon that can be ruled out as a tactic for the British police; therefore it would be a slight overstep to assume that Britain may not engage in covert, shadowy manoeuvres simply because of the implementation of the PREVENT strategy.

Nonetheless, judging by the FBI’s tactics used against Tounisi, the US is willing to encourage people into committing acts of terror in foreign countries in order to carry out sting operations. Conversely, it is crucial to bear in mind what was discussed in Chapter 4 regarding the incompatibility of ethics and intelligence. In fact, Shelton referred to the application of legality, ethics and intelligence as paradoxical (2011, p.26). While it may be ideal to try and maintain democratic ideals, to some extent, such ideals are morally antithetical with propaganda and surveillance.

These two tools (propaganda and surveillance) are used to protect democracy from the so-called *barbarians at the gate*. Perhaps the inability to apply ethics and intelligence coherently is because the state has different selves that subscribe to different standards. Although democratic institutions such as Parliamentary committees can hold intelligence services in the UK and other nations accountable, ultimately, intelligence services often engage in amoral activity for the betterment of national security and at times, for the expansion of state influence in different parts of the world.

In the case of the FBI and Tounisi, it would appear that states are willing to suspend their liberal democratic sense of self to allow its organs to carry out intelligence operations

which undermine basic (liberal) democratic values. Cognisant of chapter 3 and 4's in-depth exploration of theUSIC's multiple aggressive intelligence operations, it would also appear that America has been managing different selves for many decades. This does not bode well for the present and future of US citizens and the citizens of foreign nations that may fall prey to propaganda and surveillance campaigns.

As discussed above, it is difficult to draw a clear line between probing for information to see how dangerous this potential terrorist is, and outright encouragement by the FBI towards Tounisi to become a terrorist. Therefore, some leeway needs to be given to intelligence services when probing for information in scenarios that would appear to be deceitful. Having said this, clear examples were demonstrated in which the FBI knowingly encouraged Tounisi to trust in their plan. What remains unclear is the degree to which the FBI will use such methods for less severe crimes. Can such entrapment be used for human rights activists, journalist, or even public figures?

At this stage, such questions remain as what they are; questions rather than concrete reality. Irrespective of the ambiguity of this situation, it is clear to say that a sham universe was engineered and sustained by the FBI. Put eloquently by Ellul '[m]an will be led to act from real motives that are scientifically directed and increasingly irresistible; he will be brought to sacrifice himself in a real world, but for the sake of the verbal universe which has been fashioned for him' (1965, p.372). To a great extent, there are parallels between the actions of the FBI and Ellul's sentiment. The FBI indeed led a man to act and provided an irresistible situation in which Tounisi if successful, would have sacrificed himself in the real physical world because of the cyber sham universe.

---

## 6.4 Analysis

---

In order to ‘meet the FBI’s mission of intelligence collection’ in cyberspace, the FBI conducts joint operations with the USIC and many international allies (FBI, 2015, p.51). Albeit speculative, it is hard not to contemplate about how many of America’s foreign intelligence service partners are aware of how propaganda and deceit are woven to attain intelligence. If other intelligence services are aware of US trolls and cyber informants that are used to gather intelligence, is it plausible to assume that America’s allies in Europe and other parts of the world are doing the same? This is truly a daunting thought considering that the US has insulated itself amongst democratic partners in conjunction with authoritarian partners that are less concerned about human rights.

If various nations are propping up sham universes online, citizens around the world are genuinely sleepwalking into a digitised false reality that is antithetical with the term cyber stability. Cooperation amongst states is not necessarily a benign phenomenon, as highlighted in Chapter 2. Seen as nations are working together to maintain sham universes in secret, it becomes difficult for researchers to verify them. A future DGC may be challenging to implement if national security concerns induce counterproductive measures such as encouraging people to join terrorist organisations. What is more striking is the statistical data, which suggests that undercover sting operations are on the rise. According to Fordham Law School Center on National Security:

*‘In 2014, 33% of the ISIS-related cases involved government informants or undercover agents. However, the share of ISIS prosecutions involving FBI undercover agents or informants has since increased to 65%. For the new cases in 2017, it is even higher—83%’ (2017, p.11-12).*

The growth in numbers concerning undercover informants highlights the USIC’s willingness to construct multiple sham universes irrespective of whether they are in cyberspace or offline. Depending on how people perceive the Fordham Law Schools analysis, the FBI can be construed as damaging the prospect of establishing cyber stability predominantly due to the continuous desire to use the Internet to incite terrorism. Social media companies such as Facebook and Google have been criticised for not doing enough to take down terrorist propaganda online (Bond, 2018). However, can the same be said



for America's terrorist material? Isn't America also responsible for poisoning the well? Considering the steep rise in sting operations, to a great extent, it is almost inconceivable that nations such as the US are willing to sacrifice their sovereignty in favour of a DGC that keeps people safe online.

Although human rights have been discussed in Chapter 1, there needs to be greater scrutiny towards covert propaganda. At this stage of the debate, it is of great importance to pose the following question; did the actions of the FBI violate any of Tounisi's human rights? To begin with, of late, there have been growing concerns about the rights of citizens in cyberspace as a result of developing surveillance technologies (OHCHR, 2018[a]). In 2013 the UN General Assembly 'adopted resolution 68/167, which expressed deep concern at the negative impact that surveillance and interception of communications may have on human rights' (OHCHR, 2018[a]). UN resolution 68/167 specifically raised concerns about the capacity of governments, companies and individuals to engage in surveillance practices that 'violate or abuse human rights, in particular the right to privacy, as set out in article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights' (UN, 2014, p.1).

Although UN resolutions may not be binding, the International Covenant on Civil and Political Rights is a binding document. As it turns out, the US is a party to this covenant. Moreover, under article 17 of the International Covenant on Civil and Political Rights, no one shall be subjected to 'arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation' (OHCHR, 2019[a]). However, can it be asserted that the FBI's actions were disproportionate and violated article 17 International Covenant on Civil and Political Rights, and thereby infringed upon Tounisi's human rights and right to privacy? Without doubt, Tounisi's online communications with what he thought was a terrorist recruiter were placed under surveillance.

On the other hand, the initial interest and need to place Tounisi under surveillance was proportionate, cognisant of the fact that the FBI was previously aware of Tounis's fascination with terrorism ('United States Of America v. Abdella Ahmad Tounisi', 2013, p.5-7). Moreover, it is necessary to pivot back to the opinion of Chief Justice Hughes and emphasise that the party responsible for the instigation of criminal activity is a crucial

element for an entrapment defence (Library of Congress, 1932, p.24). As previously mentioned, Tounisi contacted the FBI via email ('United States Of America v. Abdella Ahmad Tounisi', 2013, p.20). Tounisi would, therefore, struggle to uphold an entrapment defence against the USG.

On the other hand, the potentially excessive encouragement provided by the FBI to Tounisi to travel to Syria to engage in the criminal act of terrorism may count as interference. However, it is vital to emphasise the fact that Tounisi was subject to temptation after he had emailed the FBI who were posing as terrorist recruiters. If this does not meet the entrapment requirement, the FBI's actions would be deemed as lawful and proportionate by US law and therefore may not be categorised as unlawful interference. Once again, Tounisi's previous admiration for terrorism and his eagerness to attain guidance from a terrorist recruiter is a significant sticking point that to some degree precludes any credible claim that his privacy was infringed upon.

This is not to imply that citizens forego their right to privacy and human rights once they begin to use platforms in cyberspace. Rather, I assert that the FBI monitored emails that were sent to them. Reading emails that were sent to the FBI does not unequivocally correlate with the UN's previous concerns about 'the negative impact that surveillance and interception of communications may have on human rights' (OHCHR, 2018[a]). Also, the monitoring of Tounisi to a great extent was proportionate considering that the FBI had previously interviewed him in 2012 and it was revealed that Tounisi had discussed the topic of bombing concerts and nightclubs with a friend. ('United States Of America v. Abdella Ahmad Tounisi', 2013, p.14).

Furthermore, the SA of the FBI highlighted the fact that Tounisi had made various internet searches to help spur his curiosity about jihad, martyrdom and terrorism ('United States Of America v. Abdella Ahmad Tounisi', 2013, p.15). Although the FBI had interviewed Tounisi in his home back in 2012, to which he admitted that he was assisting a friend with terrorist planning, the nature of how the FBI obtained his internet search records is slightly unclear. The SA conceded that Tounisi's online activity was subject to 'law enforcement surveillance' which indicates that online monitoring of the FBI's email box may have not been the only form of surveillance. Moreover, according to court records, 'the FBI also used FISA warrants to make cases against.... Abdella Tounisi' (Shiffman Cooke and

Hosenball, 2013). Although the privacy of all American citizens is in part ensured under the fourth amendment, it 'is not a guarantee against all searches and seizures, but only those that are deemed unreasonable under the law' (United States Court, n.d.).

Additionally, in the case of *Payton v. New York*, it was held that warrantless searches and seizures inside the home without a warrant is unreasonable under the fourth amendment ('*Payton v. New York*', 1980, p.1; United States Court, n.d.). On the other hand, in the 21<sup>st</sup> century, FISA warrants granted to the FBI enable the Bureau to carry out surveillance in the US. Tounisi's private communications and internet search history may have been violated, but it was proportionate after a FISA warrant was obtained by the FBI (Shiffman Cooke and Hosenball, 2013).

Perhaps, the FBI's actions are an affront to a subjective sense of morality and dignity but not quite a gross violation of privacy and human rights. While such measures may appear to be distasteful to some, it is difficult to claim that Tounisi's human rights and privacy have been violated. As a result, the practice of sting operations has continued to flourish within the US. In fact, in 2019, the Immigration and Customs Enforcement (ICE) alongside Homeland Security Investigations (HSI) set up fake Facebook accounts to catch eight individuals who attempted to enrol hundreds of international students into a university that turned out to be entirely fictional. Unsurprisingly this fake university was run and operated online by US operatives from HSI (US Immigration and Customs Enforcement, 2019; Holpuch, 2019).

However, The International Covenant on Civil and Political Rights clearly states that '[a]ny advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law' (OHCHR, 2019[a]). The US has ratified the International Covenant on Civil and Political Rights, but the FBI created a terrorist website online that millions of potential viewers can see. Throughout the affidavit provided by the FBI, it became clear that Tounisi was seduced by the incitement of religious hatred and discrimination towards others. Islamic extremist ideology is predicated on hatred for non-Muslims and Muslims who do not subscribe to their extremist interpretation of Islam. Despite this basic concept, the FBI decided to incite hatred online by concealing their true identity and feeding Tounisi falsehoods concerning logistical and material support to fight in the Syrian conflict.

Moreover, the original point of attraction was the FBI's fake terrorist website which promulgated war propaganda. This would suggest that the aforementioned binding covenant on civil and political rights was violated when the FBI concocted a ruse that Tounisi fell for. To date, the US has not received punishment by the international community for carrying out this particular sting operation against Tounisi. Until greater discussion takes place at the international level to provide guidance and reinforce limitations on war propaganda to members that have ratified the International Covenant on Civil and Political Rights, amoral sting operations will continue to take place in the US.

Regardless of whether it can be established that Tounisi's privacy was violated it can be asserted that the case study of Tounisi clearly demonstrates that the US created war propaganda to ensnare Tounisi and others. Attempting to portray the FBI's actions as entrapment, by American legal standards is plausible but very difficult. Presenting the US a rogue state for defying the International Covenant on Civil and Political Rights is plausible, however many nations engage in war propaganda and have a fairly nonchalant attitude about doing so ('Prosecutor v. Dusko Tadic aka "Dule"', 1997, p.36; The Bureau of Investigative Journalism, 2017). To some degree, the attitude of relative nonchalance is a result of states juggling different selves to which some (ontological self) are beholden to amoral behaviour that infringes upon the International Covenant on Civil and Political Rights. Nations often attempt to present themselves as peaceful when addressing its citizens about foreign powers. For example, President Reagan portrayed several of America's adversaries in an essentialist homogenous context whose ontological crux was permeated by a fixation with terrorism:

*Iran, Libya, North Korea, Cuba, Nicaragua . . . are arming, training and supporting attacks against this nation. And that is why we can be clear on one point: These terrorist states are now engaged in acts of war against the government and people of the United States. And under international law, any state which is the victim of acts of war has the right to defend itself... The growth in terrorism in recent years results from the increasing involvement of these states in terrorism in every region of the world. This is a terrorism that is part of a pattern--the work of a confederation of terrorist states . . . a new, international*

*version of Murder, Inc... And all of these states are united by one simple, criminal phenomenon--their fanatical hatred of the United States, our people, our way of life, our international stature* (Reagan, 1985, cited in Skelton, 1985)

In this example, President Raegan sought to shape the intrinsic nature of his list of adversaries while simultaneously omitting acts of state terrorism committed by the US. In doing so, President Reagan hoped that listeners would make the inferential leap of assuming that the US has not terrorised any groups of people or nations domestically or abroad. However, as mentioned in Chapter 1, Malcolm X previously contemplated the irony of America portraying itself as the democratic leader of the free world while simultaneously denying African Americans basic civil human rights that white Americans were entitled to.

America has a rich history of engaging in reprehensible anti-democratic acts that have created or widened the fissures between America's democratic self and its amoral self (see chapter 3). In the 21st century, the FBI and other intelligence and law enforcement services are willing to engage in acts of deception in the most undemocratic manner. This form of behaviour and lack of morality is at the crux of America's intelligence culture as well as its ontological self. Chapter 3 explores the evolution of US and British Intelligence services which revealed that the FBI targeted African American civil rights figures and groups with psychological warfare and intrusive surveillance measures. Perhaps the FBI's actions towards Tounisi should not come as a surprise, as theUSIC's history is imbued with examples of deceit.

Moreover, a considerable amount of citizens in democratic nations may still be under the impression that Western democracies do not engage in dirty tricks that are usually associated with the Soviet Union or modern-day Russia. One way to potentially mitigate OIS experienced is to eliminate the impression that Western powers do not share similar traits with authoritarian states when it comes down to counterintelligence and law enforcement investigations. In reference to Chapter 4's literature review concerning the ethics of intelligence and the democratic state, it is vital to draw insight from the previously cited words of General Doolittle. Concerned about America's fair play democratic orientation within in the early 1950s, General Doolittle argued that it was necessary to explain to the American people the necessity of understanding and accepting

the degenerate but beneficial philosophy of fighting a dirty covert war against an enemy who employs all means to threaten America's democratic existence (Office of the Historian, n.d.[d]).

To begin with, such a view underpins the anarchic impulses that seem to have been embraced by the FBI. Therefore, to avoid the existential shock or OIS that manifests when Western intelligence services are exposed, as was the case in the Snowden leaks, it might be necessary to explain to citizens that America has lowered its democratic bar. Or put slightly differently, it may be necessary to explain to American citizens that the US has different selves to which some of them are amoral but necessary to fight hostile adversaries. Paradoxically, this move has been made to preserve democracy from hostile adversaries. Those that overcome this tragic irony may feel less OIS when leaks appear that the FBI has been encouraging people to fight in Syria as a part of a wider sting operation.

Conversely, destroying the fabric of America's democratic sense of self may prove to be equally detrimental to its OS. Nations that are waging covert campaigns in cyberspace are thus trapped in a flux of OS and OIS that never ends due to the persistence of anarchy in cyberspace and offensive Realist conditions that push states into wielding dirty tricks in cyberspace. Effectively, nations that attempt to mitigate OIS in cyberspace tend to experience further OIS. The question that policymakers and intelligence services of various governments have to ponder is; should citizens be subject to high-risk litmus tests that can crystalize nefarious beliefs?

This dangerous litmus test has the potential to escape the control of the tester and spiral haphazardly within the social echo chamber of the original target who may also be just as vulnerable to terrorist inclinations. Additionally, this was a prominent issue addressed in Chapter 8, in which the Pentagon's propaganda activity and products (terrorist videos) in Iraq made its way back to the US.

---

## 6.5 Conclusion

---

In this chapter, a great deal of emphasis and questions surrounding right and wrong, morality and entrapment have been probed. By US legal standards, it would appear that Tounisi was not entrapped per se as he was previously interested in terrorism. However, it is vital to note that in the case of *Jacobson v United States* the defendant (Jacobson) had originally ordered a magazine containing nude images of teenagers. The extensive inducements against Jacobson by law enforcement operatives, on the other hand, helped to qualify his claim of entrapment. To some extent, Tounisi may very well have been subject to entrapment. On the other hand, the undeniable fact that Tounisi and an untold amount of others have been led astray by the FBI is a troubling sign for society and the integrity of cyberspace platforms. Furthermore, if people such as Tounisi are unable to claim entrapment in a court of law, this would suggest that propaganda and untruthful communication is acceptable.

To some nations, creating a fake terrorist website for the sake of national security may become the norm, as intelligence services can fall back on the claim that citizens should not be on such websites in the first place. Moreover, citizens and states may view the FBI's creation of propaganda for war to be an infringement of the International Covenant on Civil and Political Rights which prohibits war propaganda under article 20 (OHCHR, 2019[a]). Reckless state behaviour has the potential to erode any reverence for international covenants that were made in good faith to help stem violence and human rights violations which are often fuelled by propaganda.

To some, the FBI's sham universe may be unacceptable, however lies and deceit are a necessary evil to endure in order to win the war on terror. Irrespective of any critique that myself or observers can muster, what the FBI has done can be viewed as ingenious. The FBI exhausted avenues to infiltrate and attract those who if given the opportunity may choose to engage in terrorism and jeopardise national and international security. It would be a near unforgivable error if an FBI operative discovered a person inciting terror online who then went and committed an act of terror but was ignored because luring him or her into a trap is not the democratic thing to do. If those who committed the atrocities of 9/11

where targeted by the FBI and successfully arrested, the American public would feel less angered when told that 3000 lives have been saved as a result.

Moreover, if the FBI or any other foreign intelligence service had used such deceitful methods to stop the recent 2015 and 2017 Paris attacks or the 2013 US Boston bombings, sympathy for people such as Tounisi would evaporate (CNN, 2019[c]; BBC, 2015[b]; France 24, 2017[a]). In the case of Paris terror attacks, a cacophony of media voices simultaneously asked why intelligence had not previously identified the assailants (NATO Review magazine, 2015; BBC, 2016[b]; Chrisafis, 2016). National security concerns may encourage nations to continue pursuing the creation of sham universes to prevent terrorist attacks, ironically by advocating terrorist attacks.

Ultimately, if multiple sham universes begin to be exposed, citizens will start to feel that they cannot trust the environment that they are communicating in. Consequently, risk and paranoia may permeate the perception of citizens around the world. US intelligence services should reconsider the way they use dirty tricks online. Considering America's history of psychological warfare tactics used against the Black Panthers, and forgeries in Latin America (see chapter 3), it is unlikely that the US will relinquish its desire to deceive its adversaries and those who are locked in a geopolitical battle for hearts and minds.



---

## **Chapter 7 Case Study 3: Tainted Leaks, Forgeries, and Propaganda. A Case of David Satter and the French Elections**

---

Of late, Russian intelligence services have been accused of engaging in cyber-surveillance and propaganda campaigns to warp perception online (ODNI, 2017[b], p.6). Non-state groups have also been accused of working on behalf of the Russian government to carry out cyber-surveillance and propaganda campaigns (ODNI, 2017[b], p.12-13). One particular online technique of interest consists of hacking and stealing information which is edited to portray a target in a negative light, then released on social media and news outlets. During 2016, David Satter, a staunch critic of the Kremlin, was targeted by a Russian linked propaganda and surveillance campaign that used forged documents to tarnish his image. As will be discussed further down in this chapter, the process of cyber-surveillance, exfiltration of information that is edited and released for propaganda purposes is known as tainted leaks.

This chapter sets out to explore the possible ramifications that tainted leaks can have on society. Following the aims and objectives set out in Chapter 1, this case study will explore Lippmann's concept of the phantom public to assess whether or not this concept is best suited to contemporary society concerning modern propaganda and surveillance efforts. More specifically, this chapter sets out to assess whether or not society is ill-equipped to deal with sophisticated or rudimentary cyber propaganda manoeuvres postulated by intelligence services and non-state groups in the form of tainted leaks. The first stage of this chapter will briefly explore Lippmann's concept of the phantom public. Following this, I will briefly highlight how edited or forged letters were used during the Cold War by the Soviet Union and the CIA to sway perception. After this juncture, the case of Satter and tainted leaks will be presented in conjunction with analysis.

---

## 7.1 Phantom Public

---

The phantom public, as a concept is based on a litany of assumptions that revolve around the inability of citizens to compute societal affairs due to the complexity of governance and the vagaries of human perception. Due to the lack of knowledge on crucial yet capacious societal problems, Lippmann viewed the average citizen as being identical to a phantom that is barely politically conscious. To prevent the interference of inept phantoms in societal affairs, governmental employees wield propaganda to direct society to the right conclusion so that democracy can survive.

As described by Lippmann, the average citizen ‘lives in a world in which he cannot see, does not understand and is unable to direct’ (1993, p.4). The lack of understanding can be attributed to the inability to juggle continuously evolving societal and international issues. Lippmann pondered a solution to the phantom public in which education seemed a logical place to turn (2015, p.12). However, with education in mind:

*[H]e is told, in one textbook of five hundred concise, contentious pages... about city problems, state problems, national problems, international problems...banking problems ... and so on ad infinitum... But nowhere in this well-meant book is the sovereign citizen of the future given a hint as to how, while he is earning a living, rearing children and enjoying his life, he is to keep himself informed about the progress of this swarming confusion of problems (Lippmann, 1993, p.13 -14).*

Nefarious propaganda aims to deceive people with timely and well-crafted erroneous information. Education, generally speaking, seeks to counter the former and push for the truth. However, as outlined by Lippmann, it would be some feat to learn all there is to know about social, political and economic matters while living a normal life. More so, ‘if all men had to conceive the whole process of government all the time the world’s work would obviously never be carried on’ (Lippmann, 1993, p.34 -35). As a consequence of this inability to conceive the whole governmental and democratic process, citizens do ‘not know for certain what is going on, or who is doing it, or where he is being carried’ which

from Lippmann's assessment made public opinion a dangerous force that needed to be placed under control (Lippmann, 1993, p.3).

Alas, the public to Lippmann was a phantom because societal attempts to play a significant role in political decisions will end in 'failure or a tyranny... [t]he theory of democracy has not recogni[s]ed this truth because it has identified the functioning of government with the will of the people. This is a fiction' (1993, p.60-61). In summary, Lippmann concluded that 'this public is a mere phantom' due to the inability to effectively or meaningfully participate in the democratic process (1993, p.67).

---

## 7.2 A Recap of the Soviet Union and CIA Backed KGU Forgeries

---

By Lippmann's high standards, a phantom public would likely be fooled by forged documents that were being crafted by elite intelligence services during the Cold War. Forged documents became a prominent propaganda tool during the Cold War because in many cases, they were believable. The CIA viewed forgeries as 'one of the classic tools of covert psychological warfare', which encompassed black propaganda (CIA, 2016[d], p.11). Forgeries had the purpose of offering 'seemingly incontrovertible evidence of a "fact" or set of "facts" which the forger wants his target audience to believe' (CIA, 2016[d], p.11). The conceptual derivative of forgeries and edited documents falls under the Western understanding of Soviet active measures and the 'Soviet intelligence lexicon' (Kux, 1985, p.1).

Accordingly, the English phrase disinformation is the direct translation of the Russian word *dezinformatsiya* (Kux, 1985, p.1). The Soviet KGB unit and the International Information Department of the Communist Party of the Soviet Union were responsible for implementing covert propaganda or *active measures* such as forged documents (Kux, 1985, p.1; CIA, 2016[e], p.1). In 1981 the US State Department referred to active measures as Soviet operations that endeavoured to 'affect other nation's policies' (CIA, 2016[e], p.1). Such methods consisted of covert and overt activities, e.g.:

*Written or spoken disinformation... Efforts to control media in foreign countries... Use of Communist parties and front organizations... clandestine radio broadcasting... Blackmail, personal and economic and... Political influence operations... outright and partial forgery of documents; use of rumours, insinuation, altered facts, and lies (CIA, 2016[e], p.1).*

Keeping in line with the concept of Soviet forgeries, according to one CIA document, from the ‘period of 1 January 1957 to 1 July 1959, a total of thirty – six forgeries of known or apparent Soviet bloc origin were distributed to targets outside the countries in which they first appeared’ (2016[d], p.14). The predominant aim of such documents was to undermine America and her Western allies (CIA, 2016[d], p.23).

Brief examples of such letters include a forged letter from the former US President Reagan to King Juan Carlos of Spain, concerning opposition to Spain joining NATO (CIA, 2016[f], p.1). Additionally, the infamous Foster letter was supposedly authored by the US Chief of Naval Intelligence Bureau Rear, Admiral Lawrence Frost, to Indonesian rebel leader Kawilarang (CIA, 2016[g], p.4).

The letter was designed to portray the US as keen to give support to rebel leaders within Indonesia during 1958 (CIA, 2016[g], p.4). In addition, the contents of the letter were designed to provoke rebel leaders into not panicking about the USG statements concerning disapproval of the Indonesian crisis (CIA, 2016[g], p.4). The forgery also added that “‘we will continue giving assistance to you through Taiwan and the Philippines and other channel”” (CIA, 2016[g], p.4).

During the Cold War, forgery campaigns were predicated on pre-existing narratives surrounding Western domination of IR or US secret collusion with global economic elites. A documented example of this was the infamous Rockefeller letter that emerged in 1957 (CIA, 2016[d], p.32). Nelson Rockefeller allegedly wrote this letter to the then US President Dwight Eisenhower. Keeping in line with Soviet policy, the fake letter highlighted the purpose of American aid abroad, which was to further US global influence through military and political ties. The following excerpt highlights the attempts made to construe America in an unfavourable light:

Although, for instance, economic and technical aid to underdeveloped countries last year amounted to more than one billion dollars, more than half of this sum was actually devoted to three countries in which military and political rather than economic considerations [were] the determining factors. These countries were South Korea, Formosa and South Vietnam (CIA, 2016[d], p.32).

If this excerpt were authentic, it would show as a definitive fact, US ambitions to build or maintain the military, political and economic influence abroad. Moreover, considering that this allegedly came from a man of wealth, it gives the impression that economic interest groups have a significant and inappropriate impact on US foreign policy. Radio Moscow capitalised on this letter and made its assessment of the situation. As cited by the CIA, Radio Moscow stated that the Rockefeller letter “shows that the imperialist interests of Rockefeller and other U.S. billionaires decide the direction of the foreign policy of the U.S. Government, which is the fascistic executor of their wishes” (CIA, 2016[d], p.27).

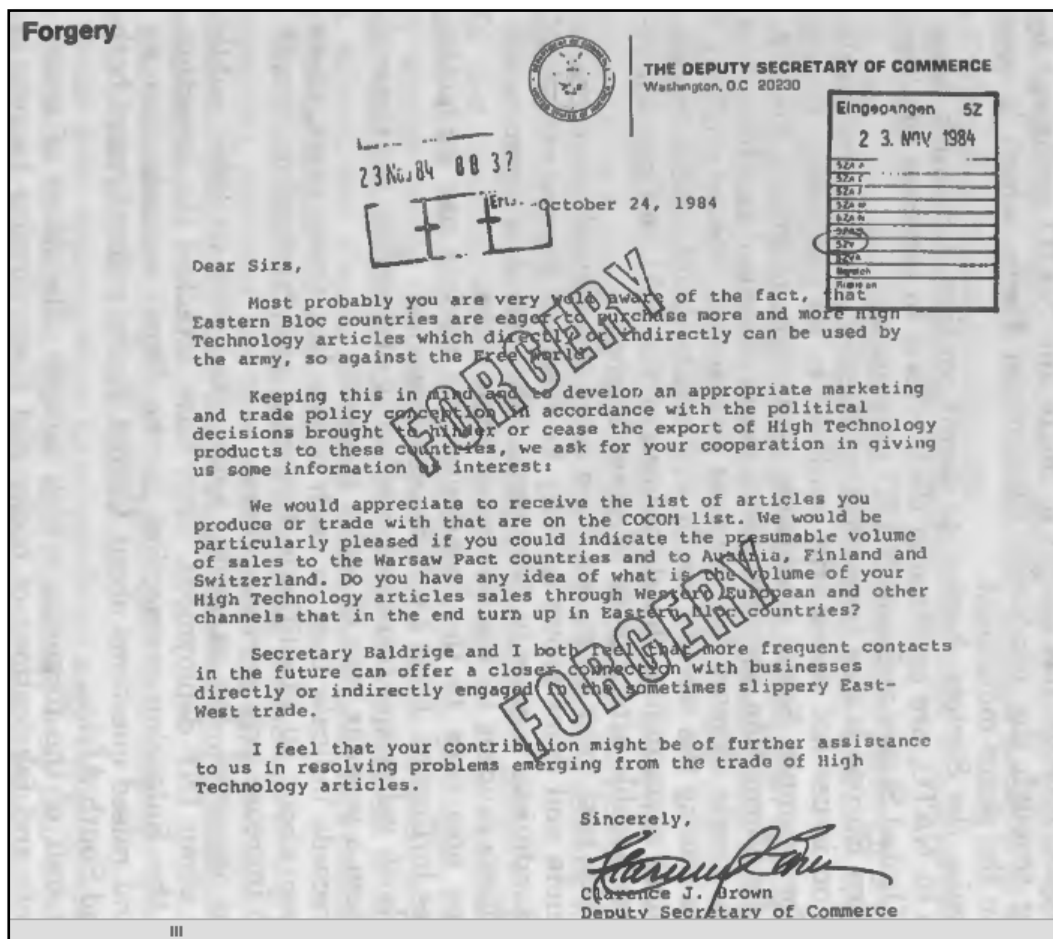


Figure 26: Library of Congress, 1985, p.13

On a social-political front, one letter of particular interest to the US was a forged KKK letter that was sent to various nations during the US Los Angeles Olympic Games. As highlighted by the CIA '[t]he National Olympic Committees of eleven Asian and African countries have recently received letters threatening the lives of their Olympic athletes' (2016[h], p.1). The nations targeted were 'Malaysia, South Korea, Sri Lanka, Zimbabwe, Senegal, Cameroon, Zambia, China, Singapore, Japan, and Hong Kong' (CIA, 2016[h], p.2). The letters described lynchings and shootings that would ensue if athletes from Asian and African nations competed in the LA games (CIA, 2016[h], p.1). The US interpreted this as a Soviet attempt to 'bolster Moscow's claim that athletes' security cannot be guaranteed at the Olympics, to reduce Third World participation at the L.A. Games, and to discredit the United States' (CIA, 2016[h], p.2). Although covert operations are challenging to prove, US reasoning at the time accused the Soviet Union of disseminating these letters because:

*None of the pro-Soviet African or Asian nations boycotting the Olympics -- North Korea, Ethiopia, Angola, Vietnam, Laos -- has received a threatening letter. The Soviets probably excluded these states as a result of receiving their firm commitment to boycott the games* (CIA, 2016[h], p.3).

Irrespective of who was responsible for the forged letters, this was an example of how fake documents can cause fear, confusion and distrust within the domestic and international arena. Judging by the wealth of knowledge and examples cited, forged letters, were a global effort to besmirch the US and its allies on a social, political and economic front. However, it is essential to note that the above examples may leave one with the impression that the propaganda manoeuvre in question emanates or is used only by Russians (Soviets).

Furthermore, history has shown that one of the CIA's most significant assets that operated in East Germany by the name of 'Kampfgruppe gegen Unmenschlichkeit [Combat group against humanity] (KgU)' under project DTLINEN used similar practices of psychological warfare (2015[b], p.1). Project DTLINEN was approved by the US in 1949 as a program to support the KgU propaganda and resistance campaign against the Soviet

Union in East Germany (CIA, 1954, p.5). DTLINEN provided support to the CIA's Berlin counterespionage and Soviet defection program that aimed to frustrate Soviet occupation of East Germany (CIA, 1954, p.9). According to one CIA document concerning the amount of propaganda material that was distributed, an estimated '327,250 pieces of material, plus leaflets produced by individual members of DTLINEN in E. Germany' were distributed (n.d., p.1).

As maintained by the CIA's archives 'DTLINEN propaganda material includes phoney letters, orders, directives purporting to be from DDR or local government officials, pamphlets and leaflets on remilitarization, unification' (CIA, n.d., p.1). Further evidence has indicated that the KGU also ran an 'aggressive economic disruption campaign' (Boghardt, 2015, p.1). During 'Operation Osterhase (Easter bunny) the KGU sent 150,000 forged letters to state-owned East German stores, ordering them to cut prices drastically, and causing a run on already scarce - consumer goods' (Boghardt, 2015, p.1). Despite the notion that the US is a democratic state that is allegedly bound to liberal notions, engaging in dirty tricks was a fundamental endeavour to curtail Soviet influence in East Germany.

---

### 7.3 Tainted Leaks

---

In the 21<sup>st</sup> century, cyber-surveillance or cyber espionage allows an individual, group or nation to illegally hack, monitor and steal large volumes of information from an electronic device. In previous chapters, it has been made clear that the CIA tasked its spies with an international surveillance remit to obtain a copy of Khrushchev's speech that denounced Stalin. Once the CIA obtained the speech, the options were to either release the document as it was, or to secrete incremental bits of information to push ideological or conceptual buttons concerning the Soviet Union. However, what the CIA did not do in that particular instance was to make changes to the content of the document. The general approach was, to tell the truth, albeit a slanted truth that fitted their pre-emptive goal of discrediting the Soviet Union. In contemporary times, hackers have chosen to digitally edit stolen documents then release them in order to sway perception in cyberspace. This has come to be known as tainted leaks, a term postulated by researchers at the Citizens Lab (Hulcoop et al., 2017).

Although attributing blame in matters of cyber espionage is very difficult to achieve, this chapter will focus on an investigation by researchers at Citizens Lab into cyber-espionage and propaganda efforts by Russian state-linked hackers against Satter. As alluded to in Chapter 1, one of the predominant objectives of this research is to assess whether or not it is logical to refer to the public as a phantom public that is ill-equipped to deal with sophisticated or rudimentary cyber propaganda manoeuvres postulated by intelligence services and non-state groups. Specifically, it is necessary to ponder whether society will succumb to the confusion created by tainted leaks and thus choose to avoid contemplating contentious issues. The work of Lippmann will be appropriated to answer this research objective. Satter is a prominent journalist who has been an outspoken critic of the Kremlin for several years. Additionally, Satter is well known for postulating and subscribing to conspiracy theories surrounding the Russian government. In particular, Satter's book *Darkness at Dawn* investigated:

*The possible 1999 conspiracy involving the Russian Federal Security Service (FSB) in a series of bombings of Russian apartment buildings that was used as a justification for the [S]econd Chechen War and which facilitated the rise to power of Vladimir Putin (Hulcoop et al., 2017).*

Consequently, Satter attracted the attention of pro-Kremlin cyber hackers, CyberBerkut, who would then later release tainted information on Satter. CyberBerkut launched a successful phishing campaign against Satter by duping him into entering his 'password on a credential harvesting site' (Hulcoop et al., 2017). As displayed in figure 27, the deception came in the form of a nefarious message stating that his password had been stolen, which required him (as a ruse) to retype his password. Once entered, the malicious actor would have access to Satter's email account. Eventually, hackers were free to explore Satter's account and exfiltrate documents.



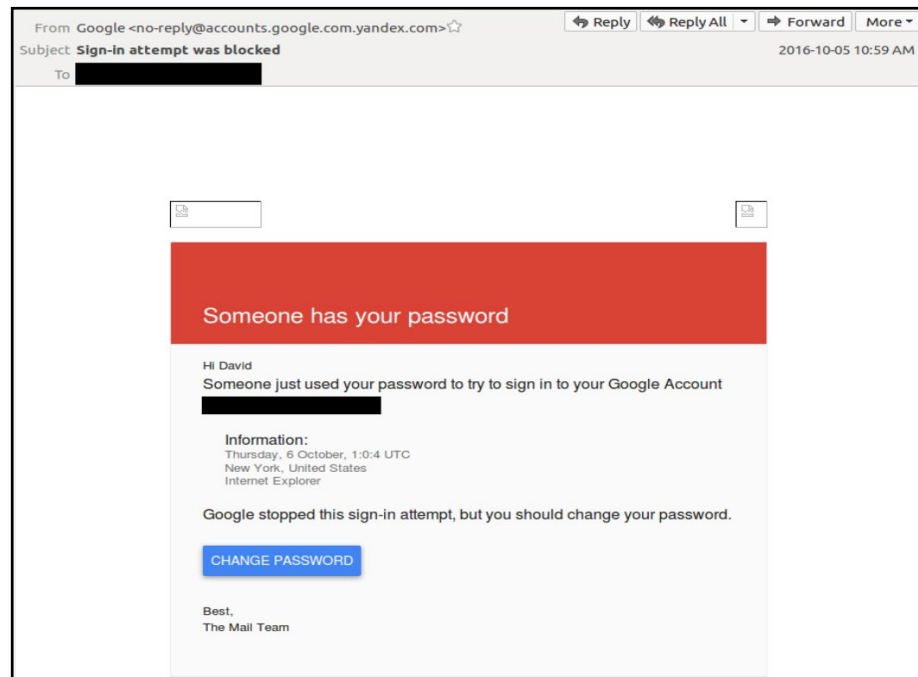


Figure 27: Hulcoop et al., 2017

Post access, a sizeable portion of documents were stolen and eventually edited to portray Satter in a negative light. CyberBerkut released deceitful edited documents to achieve this goal. Fortunately, Citizens Lab found it relatively easy to spot the manipulation by juxtaposing the original documents from Satter’s email and what CyberBerkut released. One particular document release was ‘modified to make Satter appear to be paying Russian journalists and anti-corruption activists to write stories critical of the Russian Government’ (Hulcoop et al., 2017).

Мы не забудем! Мы не простим!

Главная Новости Видео Берушкин Гуманитарная катастрофа Контакты

22.10.2016 г. Киберберкут взломал NED: США готовят "цветную революцию" в России по украинской модели

Мы, Киберберкут, получили доступ к закрытой переписке сотрудников Национального фонда демократии (NED, National Endowment for Democracy).

В 2013 году на Украине началась реконструкция, которая развела все страны, разделила семьи и разожгла гражданскую войну. Известно, что одним из главных спонсоров данного процесса шоу был финансируемый Конгрессом США Национальный фонд демократии. "Благодаря" деньгам которого многие молодые украинцы вышли на улицы и устроили погромы.

Тогда американцы действовали по отработанной схеме: сначала подогрели общественность публикациями в финансируемых ими СМИ, а потом уже в открытую стали "включать" деньги в проекты на улицах. Сейчас же этот фокус пытаются повторить с Россией. И одну из главных ролей в этом играет журналист Димитрий Саттар.

По информации у нас информации, Саттар работает на американские спецслужбы и поддерживает тесные связи с международным аферистом Уильямом Бурдском. Саттар долгое время жил в Москве и сотрудничал с тремя изданиями, как Wall Street Journal, Financial Times и "Радио Свобода". Однако с 2013 года ему было отказано в приеме российской визы. С тех пор он и начал активно поддерживать российские оппозиционные СМИ.

Как удалось выловить из материалов NED, г-н Саттар оказывает весьма широкий спектр услуг. Если изучить все отчеты, становится ясно, что чуть ли не каждый авторитетный пропагандистский материал, который публикует "Радио Свобода" и ряд российских "либеральных" СМИ, готовится под чутким руководством Саттара.

Только за первые десять месяцев 2016 года по заказу г-на Саттара было подготовлено 24 статьи и журналистских расследований в таких СМИ, как РБК, "Ведомости" и "Радио Свобода". Например, материал Сергея Диброва "Черный день в истории Одессы", который оскорбляет память людей, погибших в Доме Профсоюзном. Еще шесть статей находятся в процессе редактирования либо готовы к публикации.

Главной задачей этой "журналистики" является дискредитация руководства Российской Федерации, членов их семей и ближнего окружения. Чаще всего в материалах, заказанных Саттаром, фигурирует Владимир Путин, Сергей Чемезов, Дмитрий Погозин, Сергей Шойгу, отец и сын Воробьевы, братья Ротенберги и другие известные россияне.

Российская Федерация: проект по разведке информации и производству пропагандистских материалов. В этом отчете, в котором содержится информация о работе офиса по борьбе с Россией, приводятся следующие сведения:

В течение первых десяти месяцев 2016 года, наряду с другими проектами, в которых были опубликованы материалы, в том числе, на сайте, опубликованы материалы по программе на английском языке. Следующий список статей был опубликован 20 октября 2016 года.

1. "The New Yorker: "Russia's Repression for Progress," January, 2016 (Interpreted on the Atlantic website) (PDF FILE)
2. "The Atlantic: "The Russian and Polish of Cyberwar," February, 2016 (for US and UK of an open source) (PDF FILE)
3. "The New Yorker: "Russia's A to Z," March 1, 2016 (for sites of Russian open source) (PDF FILE)
4. "The Atlantic: "Russia's A to Z," March 20, 2016 (for sites of Russian open source) (PDF FILE)

Figure 28: Hulcoop et al., 2017

To aggrandise the potency of this campaign, anti-Western, interventionist narratives were apotheosised when Russian state-owned media began to report this leak as something credible. Russian state-owned news outlets such as RIA Novosti, and Sputnik Radio; 'picked up the narrative, and gave voice to a number of sources who claimed that the "leak" was evidence that the United States Central Intelligence Agency (CIA) was attempting to foment a "colour revolution"' (Hulcoop et al., 2017).

Unsurprisingly the alleged leaked document was referenced in Russian state TV as legitimate proof of attempts 'to discredit the Russian president' (Hulcoop et al., 2017).

---

## 7.4 Analysis

---

As previously mentioned, the goal of this chapter is to dissect and assess the concept of OIS in conjunction with Lippmann's conception of the phantom public. Lippmann's bleak view of public opinion serves to illuminate the issue with tainted leaks in a digital era that is at risk of becoming accustomed to the regular dissemination of propaganda. The significance of this case study lies behind the aura and perception of noble hacktivists that are exposing hidden truths in a disinterested way. Followers of such groups may unwittingly follow the narrative of hacktivist who have premeditated goals of influencing the public into a conclusion about Satter and the foreign policy of Western nations. The danger concerning public opinion is that followers or phantoms are dependent on indicators from disingenuous groups that are secreting black propaganda as opposed to waiting on a multitude of independent researchers such as the Citizens lab to verify the leaks. In this scenario, according to Lippmann, the public 'can watch only for coarse signs indicating where their sympathies ought to turn' (1993, p.54).

Waiting for cues is a direct result of members of the public lacking 'insider's knowledge of events' (2015, p.54). News stations in many respects play a role as the guardians or shapers of public opinion, yet if the public is always on the exterior being connected to reality by a biased or unwitting intermediary, to what extent can citizens be appropriately informed about faraway issues on a daily basis? Without direct knowledge of evolving situations or the capacity to be an omniscient citizen, to some extent, members of the public are relegated to phantom-like states, swayed by the signals of a distant propagandist. This assessment proposes a fundamental problem. At this juncture, citizens who are concerned about Satter's leaks may be focused on the authenticity of the source as opposed to critically assessing the truth.

In the event that some citizens are unable to verify the integrity of the sources intention and the contents of the leak, perception of the truth is pegged to the side that can push a significant amount of convincing information via social media and news stations. Journalists such as Satter find themselves in an uphill battle attempting to compete with the information capacity of Russian state news, CyberBerkut and their obedient phantom-

like trolls. Considering the lack of time working individuals can give towards verifying news sources, the volume of sources saying the same thing can give the illusion that the truth has been identified.

In Lippmann's view, 'the citizen gives but a little of his time to public affairs, has but a casual interest in facts and but a poor appetite for theory' (Lippmann, 1993, p.14-15). Consequently, those that are already in orbit of conspiratorial narratives may not see the need in confirming the facts but simply adhere to the message that CyberBerkut presents. Therefore, it is easy to assume that those who are under the gravitational pull of propaganda cannot escape its orbit due to Lippmann's suggestions about the phantom public.

On the other hand, Alexei Navalny, a Russian anti-corruption activist who was also the target of CyberBerkut's tainted leaks campaign presented a viewpoint that is halfway between Lippmann's bleak view and the acknowledgement that people can be dissuaded from propaganda. According to Navalny '[a]t the end of the day everyone will understand — documents are fake, but it will be a two-week-long discussion: '[i]s [the] opposition and Navalny in particular using Soros' money?'' (Navalny, 2016, cited in Groll, 2016). A substantial amount of doubt has still not been extirpated from the picture that Navalny presented, which leaves citizens open to propaganda and confusion. In addition to the issue of citizens needing to be connected to broader social affairs, a consequence of this problem is that people are continuously walking into the scene of events then leaving before all the facts have been established.

Individuals who were previously unequipped with all the facts or the means to digest them are given information to take on board, before the news shifts to a completely different topic that requires a new set of lens to inspect the matter at hand. Accordingly, it can be asserted that '[t]he public will arrive in the middle of the third act and will leave before the last curtain, having stayed just long enough perhaps to decide who is the hero and who the villain of the piece' is (Lippmann, 1993, p.55).

Placed in a real-life scenario, the public arrives during the leaks and in many cases leaves once clicking off the CyberBerkut website or watching Russian state news. Irrespective of whether an observer of tainted leaks is an advocate of CyberBerkut and Russian state

news or not, it is inevitable that some may stumble into propaganda and fail to decipher between truth and fiction. As a consequence of arriving at tainted leaks during the third act, it is possible that some may choose to exit the scene with CyberBerkut's narrative as a potential truth due to the time constraint of needing to juggle leaks with other stories before returning to normal daily activities.

If enough momentum is built up concerning the forged document, particularly from media outlets, the underlying goals of the propagandist can be attained. In the case of the CIA's anti-Cuban forgeries in Peru, the public did not overwhelmingly warm towards the forgery. Eventually, enough momentum was gathered that the government of Peru severed diplomatic relations with Cuba (Agee, 1975, p.121) (see chapter 3).

However, in the modern information era, the transmission of ideas within cyberspace is so powerful that even if mainstream news stations do not emphasise the leaks on Satter, the damage could be done online with little direction from the original source. The danger that cyberspace provides is that at any point in location or time, a conspiracy can be generated and regenerated throughout various echo chambers without direction. In other words, the propagandist can launch a campaign that takes a life of its own and no longer needs direction from the source. Unwitting observers who are at the time unaware of the logistics behind the tainted leaks campaign may stumble into half-truths or outright lies. As such Lippmann summarised this viewpoint with the poignant analogy of the 'the fable of the pensive professor walking in the woods at twilight':

*He stumbled into a tree. This experience compelled him to act. Being a man of honor and breeding, he raised his hat, bowed deeply to the tree, and exclaimed with sincere regret: "Excuse me, sir, I thought you were a tree." Is it fair, I ask, as a matter of morality, to chide him for his conduct? If he had encountered a tree, can any one deny his right to collide with it? If he had stumbled into a man, was his apology not sufficient?... You may retort that he had a moral obligation to know the difference between a man and a tree... But suppose that instead of walking in the woods he had been casting a ballot (Lippmann, 1993, p.18-19).*

With so much information present, citizens at times cannot help but stumble into false pretences and mistake it for the truth. In the case of Soviet forgeries in the US, it was

inevitable that some would believe in the fake letter that was allegedly written by the KKK due to the racist climate that many African American's were subject to. Similarly, pro-Kremlin Russian citizens who were aware of Satter's anti-Kremlin journalism at the time of the RIA Novosti news report may have been swindled by disinformation, due to the underlying theme of an anti-Kremlin individual finally being *caught out*.

Irrespective of whether or not people subscribe to the idea of a phantom public, continuously or even occasionally walking into *trees* may in time or at present lead to strong opinions on leaks and intelligence matters being curtailed. Amidst the confusion about whether or not forged documents are real, the overwhelming fact that citizens are dependent on news stations for information to which at times, are seemingly incapable of unequivocally reporting the truth, may push people away from holding strong or even moderate political views. In short, sentiment on issues can become severed.

In replacement, to make up for the risk of believing in the news that is later debunked, some may choose to embrace the neutral stance of *who knows?* Ultimately, the average citizen might feel ashamed that they publicly or privately proselytised erroneous stories only to realise a distant propagandist has deceived them. Anxious about being wrong for a second time when presented with a new set of leaks or the news in general, OIS can push citizens to abandon their tendency to hold strong opinions or any opinion. The future of public opinion is at risk of being culled by OIS, which can:

*[C]ontribute to cynicism about the media and institutions at large as being untrustworthy and unreliable, and can cultivate a fatigue among the population about deciphering what is true or not. By propagating falsehoods, the aim is not necessarily to convince a population that the falsehood is true (although that outcome is desirable) but rather to have them question the integrity of all media as equally unreliable (Hulcoop et al., 2017).*

As a result of this, Neil MacFarquhar has commented on the issue, stating that confusion can 'foster a kind of policy paralysis' in which people become confused and overwhelmed by the endless possibilities that both sides of the debate could be trying to deceive the subject (2016). Consequently, the individual's stance on the matter and potentially other issues become frozen or betwixt in confusion and mistrust for information due to the

concern that it is difficult to comprehend the litany of points and counterpoints. This situation is inflamed by news stations that are caught releasing propaganda that is later proven to be false. In a post-revelation scenario in which Citizens Lab have juxtaposed real and fake documents, viewers may not be confident in trusting the guardians of knowledge, i.e. news stations such as RIA Novosti.

Within this atmosphere of distrust, tainted leaks can leave portions of the public betwixt in a cognitive state of knowing and not knowing. As a direct consequence of being in a state of flux over contentious events or as Lippmann put it a 'bewildered as a puppy trying to lick three bones at once', citizens will offload this cognitive burden by partially or entirely withdrawing from the issue at hand (1993, p.15). Far from being a one-off attempt, tainted leaks and online releases of information are chipping away at the threshold or tolerance levels of accepting digital leaks. Ordinarily, this would be a good thing if people simply chose to ignore propaganda and only focus on factual information.

Unfortunately, the information environment is not as simple as this. Should another situation arise in which a purported leak or *evidence* is presented, the cycle of the confusion starts all over again. For example, the infamous *Steel dossier* authored by former MI6 officer Christopher Steele was published by mainstream news outlets without the document being confirmed as a definitive body of facts. This scenario left the public mystified as to whether its content is worthy of condemning President Trump (The Washington Post, 2018).

This issue is further compounded by the level or frequency of events that are taking place which revolve around dubious leaked documents and emails in the 21<sup>st</sup> century. At present, Saudi Arabia and its allies have maintained an air land and sea embargo on its neighbour Qatar, predominantly due to a leaked email which purportedly showed Qatar's support for Iran as an Islamic power (DeYoung and Nakashima, 2017). While it is dangerous to flirt with the use of opaque sources that official US representatives have not confirmed, it is essential to highlight that The Washington Post cited unnamed US intelligence officials in saying that:

*The United Arab Emirates orchestrated the hacking of Qatari government news and social media sites in order to post incendiary false quotes attributed to*

*Qatar's emir, Sheikh Tamim Bin Hamad al-Thani, in late May that sparked the ongoing upheaval between Qatar and its neighbors (DeYoung and Nakashima, 2017).*

Instinctively, Qatar has denied the validity of leaks with a rebuttal that highlights the key talking points of this chapter. As such, the Qatari government has claimed that the purported leaks are a part of a “well-coordinated smear campaign designed to damage the image and reputation of Qatar. And the smear campaign, in turn, set the stage for the blockade and the ultimatum that followed in June” (NBC NEWS, 2017). Elsewhere in the world, other examples of edited leaks include the campaign against Hillary Clinton, United States Agency for International Development (USAID) in Armenia (see figure 29) and the US embassy in Moscow. In the case of the latter, Russian newspaper Izvestia published a fake embassy letter which implied that ‘the US pays gay rights activists to smear Russian officials’ (Luhn, 2015).

On the contrary, it must be noted that the extent to which OIS has had an impact on public opinion is yet to be determined or quantified. In the case of the USAID forgery, the US embassy in Armenia responded on Twitter with humour and pointed out the misspelling of sincerely with ‘Sincelery’, ‘Sin + celery? ... USAID is in fact a big fan of celery, and indeed of all vegetables’ (see figure 29) (US Embassy Yerevan, 2017, cited in Nimmo and Barojan, 2017).



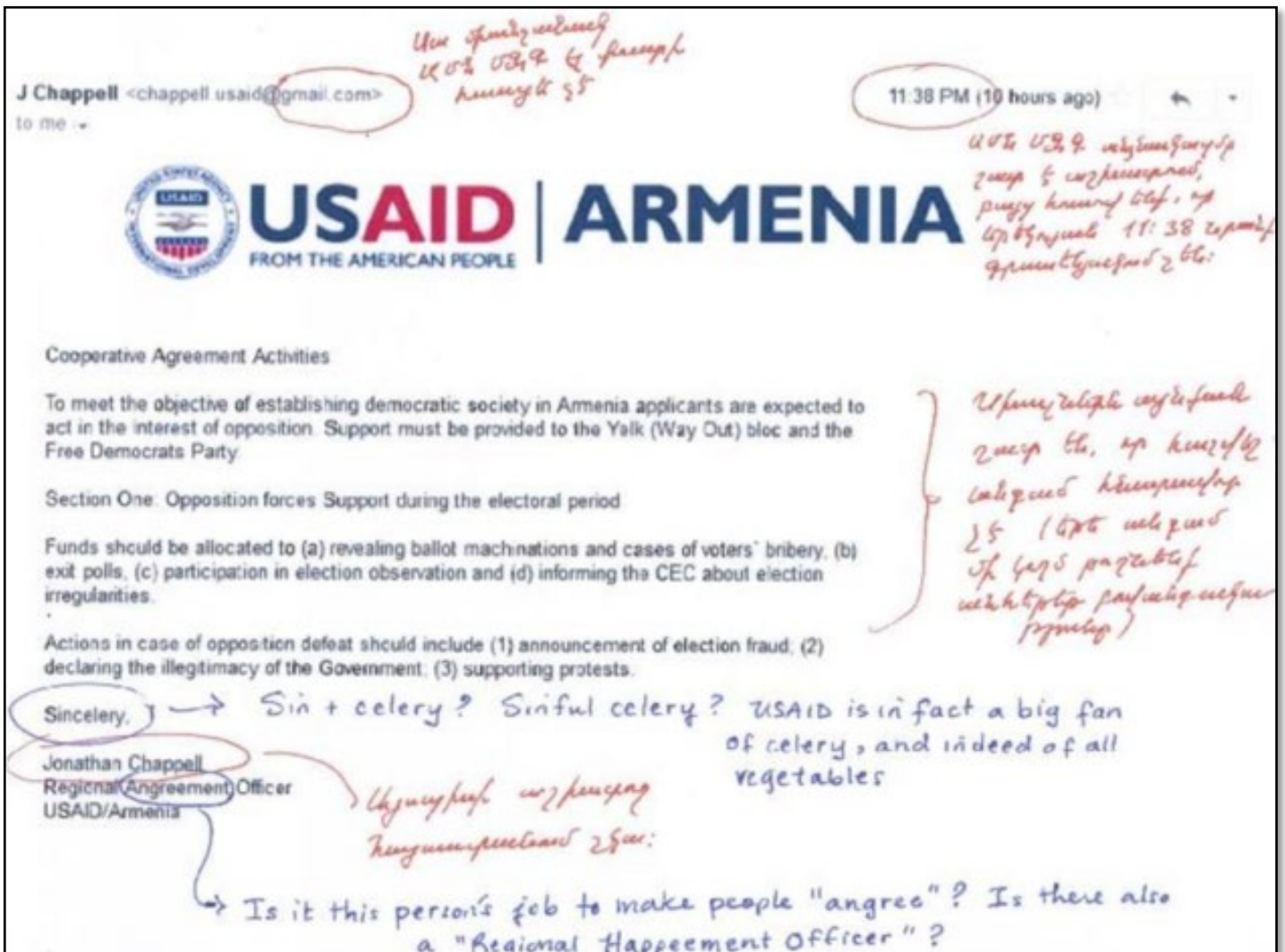


Figure 29: US Embassy Yerevan, 2017, cited in Nimmo and Barojan, 2017

Similarly, the US embassy was quick to remind the propagandist behind the fake documents that, ‘Armenians are too smart to fall for such silly games?!’ (US Embassy Yerevan, 2017, cited in Nimmo and Barojan, 2017). Other cases of tainted leaks have not brought about the same vortex of confusion compared to the collection of dirty tricks used in the US 2016 election. As a result, it may be a cavalier move to assume that populations who are subject to tainted leaks cannot see through propaganda. Therefore, the generalisability of the term phantom public in many respects is relative and limited to small portions of people. Conversely, this does not dispel the potential for a tainted leaks

campaign to be successful in the future, particularly if this is carried out by a nation-state, as was the case during the Cold War. So far, this chapter has encompassed a very pessimistic and condescending tone without much substance to qualify all of Lippmann's claims. Literature cited from Lippmann's book *The Phantom Public* primarily revolves around the assumption that the average citizen is ill-equipped to deal with public affairs. Lippmann is therefore opposed to the concept of an omniscient citizen existing in large modern cities and towns.

As highlighted in Chapter 4 '[t]he ideal of the omniscient, sovereign citizen is... such a false ideal. It is unattainable. The pursuit of it is misleading' (Lippmann, 1993, p.29). While producing a perfect being is off the table at this moment in time, hacktivists failed at their opportunity to significantly influence the perception of French citizens during the 2017 French presidential election. This was primarily because citizens may not be as vacuous as Lippmann pictured. Judging from the results and the overall French reaction to tainted leaks, it is not unreasonable to suggest that the threat of OIS, actually brought about OS and a strong will to rebuke the leaks targeted at President Macron. This indeed may have been a surprise to Lippmann.

At the climax of the French election, President Macron's campaign team was targeted by a cyber-attack which has been attributed to Pawn Storm also known as Fancy Bear or APT28 by cybersecurity firm Trend Micro (Auchard, 2018; Trend Micro, 2017). Experts at Trend Micro noted that 'Pawn Storm's activities show that foreign and domestic espionage and influence on geopolitics are the group's main motives, with targets that include armed forces, the defense industry, news media, and politicians' (2017). A sizable amount of documents were released on to the Internet hours before the debate between President Macron and his opponent Marine Le Pen.

Tainted documents alluded to the alleged existence of a secret offshore account owned by President Macron (France 24, 2017[b]). At the time, Marine Le Pen breathed further life into the leaks by commenting on them during the live televised debate "I hope we will not find out, Mr Macron, that you have an offshore account in the Bahamas" (Le Pen, 2014, cited in France 24, 2017[b]). Following this public swipe at President Macron the

#MacronLeaks campaign on Twitter was beginning to simmer reaching ‘47,000 tweets in just three and a half hours after the initial tweet’ (Nimmo, et al., 2017).

Despite the initial surge in chatter on social media, the leaks were quickly outed as a malicious attempt to disrupt the French elections. President Macron went on to win the presidential election by a considerable margin, bringing the potency of tainted leaks and Lippmann’s concept of the phantom public into disrepute. So how is it that in Chapter 5, the US elections produced a significant amount of OIS, but in the French elections tainted leaks had a limited impact?

Aside from the obvious lie that was construed in an attempt to suggest financial wrongdoings on President Macron’s part, I point to the US 2016 election experience that the world witnessed. In the aftermath of the US elections, European nations were alert and on guard for any similar attempts to divide countries over leaks. Also, the French were prepared by incoming intelligence from the NSA and reacted quickly to the tainted leaks. In the words of the then NSA chief, Adam Rodgers:

*We had become aware of Russian activity, we had talked to our French counterparts prior to the public announcements of the events that were publicly attributed this past weekend and gave them a heads up, look were watching the Russians were seeing them penetrate some of your infrastructure. Here’s what we’ve seen, what can we do to try and assist. We’re doing similar things with our German counterparts, with our British counterparts they have an upcoming election sequence. We’re all trying to figure out, how can we try to learn from each other (CNN, 2017[c]).*

In order to act upon this information and the release of propaganda, the French government warned that the promulgation of material online would likely fall under criminal law, thus acting as a swift legal deterrent (Commission Nationale de Contrôle de la Campagne électorale en vue de l’Élection Présidentielle, 2017). From one angle, the US election has inoculated the rest of the world and serves as an example of what can happen if information or propaganda via leaks is not distinguished effectively. While various echo chambers will still welcome conspiratorial information that is predicated on tainted leaks, wider society to an extent has adapted to tainted leaks and dirty tricks. In

the aftermath of the French experience in 2017, John Hultquist, the director of cyberespionage analysis at FireEye has alluded to the notion that '[t]he only good news is that this activity is now commonplace, and the general population is so used to the idea of a Russian hand behind this, that it backfired on them' (Hultquist, 2017, cited in Nossiter, Sanger and Perloth, 2017). Overall, the French were able to appraise the situation, whereas Lippmann was adamant that citizens 'cannot, therefore, construe intent, or appraise the exact circumstances...of the... argument' (1993, p.54).

In the future, more sophisticated campaigns may make it harder for a phantom-like public, far removed from events, to have a positive or negative opinion on a particular event. It is vital to remember that Blum pointed out that the CIA bombed churches in the past and made the act seem to have been committed by someone else (2003, p.173). Similarly, it is crucial to remember that forged CIA documents encouraged the nation of Peru to break diplomatic relations with Cuba (Blum, 1986, p.191). If a professional organisation or elite intelligence services were to provide convincing tainted leaks that can dupe people worldwide as staged propaganda has done in the past, online platforms are in danger of descending into a constructed sham universe.

Before bringing this chapter to a close, it is fundamental to emphasise the notion of anonymity. Many non-state groups that claim to be hacktivists are anonymous individuals who engage in the illegal theft of documents from networks. The cover of cyberspace allows groups or individuals to evade punishment from law enforcement agencies. CyberBerkut acts outside of the law and therefore cannot be controlled until the police or an intelligence service catches them. Anonymity has been the greatest strength of hacktivism, which is supplemented by cyberspace. If states will find it hard to submit to the DGC, it is difficult to envision how non-state groups will also end their reckless acts of undermining network security of the state and citizens around the world. Both state and non-state groups puncture cyber stability. EI or hacking remains a fundamental tool that enhances propaganda campaigns around the world.

---

## 7.5 Conclusion

---

To conclude this chapter, it is apparent that the word, fact, is losing credibility as a word that can describe information concerning societal affairs. Consequently, hackers and governments have preyed upon this element of doubt, which has impacted countless amounts of international and domestic crises. In today's world, tainted leaks that purport to expose something ominous about a target serves the purpose of discrediting people, nations and organisations, but can inadvertently lead to confusion and OIS irrespective of whether the truth is discovered. The space between facts, half-truths and lies has created a breeding ground for conspiracy theories to grow.

Most importantly, this space has paved the way for non-state groups to appropriate the ability to push false narratives. Lay individuals, far removed from the source of the event, at times can feel like disorientated victims caught up in the battle of hearts and minds. Until messages can be verified as facts, society must appreciate and accept that at times citizens will walk into *trees* and mistake them for humans as pointed out by Lippmann.

In other words, the truth is just as polymorphic as the vagaries of human perception. Having reviewed the evidence cited in this chapter, it would appear to be inappropriate to use the term phantom public to generalise society. The French elections (as a subcase study) demonstrated that tainted leaks had a limited role in the electoral process and public opinion in general. While the term phantom public does hold true in certain circumstances, tainted leaks by CyberBerkut has not had the same impact as the propaganda campaign witnessed during the US 2016 presidential elections.

Perhaps future researchers should probe those who viewed tainted leaks and still hold them as truths. Similarly, it would be wise for future researchers to investigate those who once believed the accusations levelled at Satter by Russian state media and now distance themselves as a result of evidence provided by Citizens Lab. Moreover, it is important to note that propaganda methods are not sedimentary. Propagandists that are aided with technology will always find a way to subvert reality and bring temporary experiences of cyber stability into chaos. Different nations may be on guard against tainted leaks, but other methods will develop and be weaponised in cyberspace. Deep Fakes and ephemeral

propaganda have already caught the attention of researchers (Dack, 2019; Langston, 2017; Wakefield, 2018; Suwajanakorn, Seitz and Kemelmacher-Shlizerman, 2017, p.1-3; Lim, et al., 2019). To this end '[p]ropaganda will never die out. Intelligent men must reali[s]e that propaganda is the modern instrument by which they can fight for productive ends and help to bring order out of chaos' (Bernays, 2005, p.168).

---

## Chapter 8 Case Study 4: Staged Psychological Warfare and Constructed Realities

---

From North Korea to Iraq constructed psychological realities have played a vital role in the battle for hearts and minds throughout military conflicts. During times of war, the domestic population must be guided into grasping certain conclusions about the causes of war and the ‘justness of one’s own cause’ (Welch, 2014). Failure to achieve support for violence domestically and in the nation under siege may incite the withdrawal of occupying troops and embolden enemy forces. Shaping the conflict and the enemy is paramount to the success of any military campaign. At times, nations choose to engage in atrocity propaganda to incite the felling of shock and communicate to foreign and domestic audiences the need to support the war.

During WW1, atrocity propaganda played a vital role in allied forces that sought to portray Germany’s invasion of Belgium in a barbaric and deplorable manner. According to the National Archives (UK) ‘[d]uring the autumn of 1914, the British Foreign Office received’ reports concerning ‘fleeing British subjects and Belgian refugees’ (n.d.[b]). This prompted Lord Bryce to publish a report on the matter which encompassed accusations of German troops ‘raping women and girls; using civilians as 'human shields' during combat; and cutting off children's hands and ears in front of their horrified parents’ (National Archives (UK), n.d.[b]). Upon discovery that the accounts of propaganda were fictitious, black propaganda became slightly more undesirable. However, several decades later, communist propaganda emanating from North Korea, China and Russia concerning alleged US BW activity was used to construct anti-American sentiment in Asia and around the world. North Korea staged and created false plague regions of infection while very little evidence was provided concerning accusations of German troops ‘boiling corpses to make soap’ in WW1 (Wilson Center, 1953[a], p.1; Welch, 2014).

The North Korean regime staged their form of psychological warfare with human bodies. Staged psychological warfare is of great interest as those responsible are creating drama like realities that will inevitably grasp the attention of the target audience. In the case of the US, two disastrous multi-trillion dollar wars in Iraq and Afghanistan has limited

America's ability to explain its narrative concerning aggressive military actions, without evoking resentment in different parts of the world.

As a result, the secretion of selective visual and audio-based content surrounding US motives is crucial for the justification of warfare. In contemporary times, the US edited terrorist videos to support its war effort to dislodge Al-Qaeda from Iraq. To be precise, the Pentagon paid UK PR firm Bell Pottinger to create terrorist and anti-terrorist propaganda videos that appeared in local media and on disks that could only be watched while connected to the Internet. Other propaganda videos appeared in local media. Such videos were aimed at silencing local support for Al-Qaeda. Knowledge of this came to light via two primary sources.

A former employee tasked with editing the fake videos and Lord Bell, the former chairman of Bell Pottinger. According to Lord Bell, the propaganda campaign in Iraq was a covert operation (Fielding-Smith, Black and Ungood-Thomas, 2016). Although, Christopher Paul has suggested that '[i]n truth, the vast majority of contemporary PSYOP are based on wholly truthful information', Bell Pottinger, knowingly fabricated its products before sending them to General David Petraeus, who also knowingly signed them off before release to various media outlets in Iraq (Paul, 2010).

This chapter sets out to highlight how modern states are adapting old propaganda methods of stage atrocities. Furthermore, this case study endeavours to highlight the consequences of failed black propaganda practices. This section seeks to explore the dangers that countries face once covert propaganda and surveillance campaigns become public knowledge. To begin with, I will highlight the historical significance of staged propaganda during the Korean War. Following the exploration of staged North Korean Propaganda, I will dissect and analyse US efforts to stage opera-like propaganda segments for Iraqi media and anti-terrorist videos during the Second Gulf War in Iraq through British PR firm Bell Pottinger.



---

## 8.1 North Korea Psychological Warfare

---

Following North Korea's decision to invade South Korea on the 25 June 1950, the UN Security Council approved the first deployment of UN forces led by America to repel the attack (Wilson Center, 2011). Professor Elliot Cohen summary of the Korean War has indicated that initially, North Korean forces 'offered a stubborn resistance'; however, after heavy fighting, the North Korean People's Army (NKPA) were driven out of South Korea (Cohen, 2016, p.2). Moreover, Cohen indicated that after heavy fighting the 'North Korean capital, Pyongyang, fell and preparations began for a drive farther north' by the US (2016, p.60).

Upon reaching close to the North Korean border (with China), China entered the Korean War and helped to push UN forces 200 miles south (Cohen, 2016, p.61). In an attempt to obtain the moral high ground during the conflict, North Korea, Russia and China wielded claims that America engaged in BW in 1951 and in 1952 (Wilson Center, n.d.).

Furthermore, in the view of the CIA Chinese Communist Premier Chou En-Lai suggested the alleged 'American use of BW [biological warfare] was aimed at "wrecking the armistice talks in Korea, prolonging and expanding the aggressive war in Korea, and the instigating of new wars"' (CIA, 2016[i], p.2). News of alleged US BW in Korea was spread throughout the world (Leitenberg, 2016). Moreover, US BW was alleged to have encompassed insects (Leitenberg, 2016). On February 21, 1952, Mao Zedong, sent a cable to Stalin, stating that:

*Over the span of twenty days, starting from 28 January to 17 February 1952, the enemy on 8 occasions used aircraft and art[illery] shells to drop three kinds of insects—black flies, fleas, and lice—on the positions of our troops in the central sector of the Korean Front around the Isen-Heiko-Sakunei Triangle, and also intermittently in the eastern sector of the front (Wilson Center, 1952 p.2).*

Furthermore, according to Wu Zhili, the former Director of the Chinese Army Health Division during 1952, 'almost all units sent telegrams of similar discoveries (within two months there were close to a thousand reports), reporting that the enemy dropped all kinds of things, including dead rats, flies and large mosquitos, vessels with insects' (Wilson

Center, 1997, p.2). Additionally, ‘one or two units reported that some North Korean citizens had suddenly died. [There were also] reports that large amounts of dead fish floated up in the river’ (Wilson Center, 1997, p.2). To some extent, the North Korean regime was genuinely suspicious of BW since American troops had experienced strange deaths. As a result, the US armed forces ‘sent Japanese bacteriological war criminal and former head of Unit 731 Ishii to North Korea to investigate this matter and publish this information’ (Wilson Center, 1997, p.2). This was a particularly sensitive occurrence as US intelligence had previously concluded that ‘twelve field trials were conducted against Chinese civilians and soldiers’ by Japan, in conjunction with the fact that General Ishii was ‘writing a treatise on the whole subject’ (Cunliffe, 2016, p.47-48).

This temporal coincidence excited the minds of the North Korean regime who ‘determined that the U.S. military was conducting bacteriological warfare’ (Wilson Center, 1997, p.2). On the contrary, to bolster support for North Korea’s war effort against the UN and American forces, Pyongyang created false sites in which bodies of victims were allegedly infected. Knowledge of this has been ascertained from declassified documents obtained by the Wilson Center. According to one document, Lt. Gen. V.N. Razuvaev explained the steps taken to infer that the US engaged in BW:

*With the cooperation of Soviet advisers a plan was worked out for action by the Ministry of Health. False plague regions were created, burials of bodies of those who died and their disclosure were organized, measures were taken to receive the plague and cholera bacillus. The adviser of MVD [Ministry of Internal Affairs] DPRK proposed to infect with the cholera and plague bacilli persons sentenced to execution, in order to prepare the corresponding [pharmaceutical] preparations after their death. Before the arrival of the delegation of jurists, materials were sent to Beijing for exhibit (Wilson Center, 1953[a], p.2).*

This was confirmed in a second declassified document, which highlighted that:

*[T]wo false regions of infection were simulated for the purpose of accusing the Americans of using bacteriological weapons in Korea and China. Two Koreans who had been sentenced to death and were being held in a hut were infected. One of them was later poisoned (Wilson Center, 1953[b], p.2).*

To compound this theme further, Selivanov, a former adviser to the Military - Medical Department of the Korean People's Army reveals in one document 'how he falsified an outbreak and blamed it on American bacteriological weapons' (Wilson Center, 1953[c], p.1). Selivanov previously admitted that '[e]arlier, already in 1951, I helped Korean doctors compose a statement about the spread by the Americans of smallpox among the population of North Korea' (Wilson Center, 1953[c], p.2). Judging by the evidence presented above that has been pooled from troves of declassified documents, it is apparent that the North Koreans, were eager to stage events to create a new psychological reality to disparage the image of the US.

In the next section, I will demonstrate how the US, a democratic country, eager to puncture regional and international support for the terrorist group, Al-Qaeda, also made use of terrorist propaganda during the second Gulf War and attributed it to Al-Qaeda. This was done for the sake of psychological warfare purposes which like the North Koreans undertook significant measures to make their product look authentic and realistic. Furthermore, this chapter will meet the objective of demonstrating that when Western democratic states attempt to employ modern surveillance and propaganda measures, they are at risk of agitating there already fragile sense of OS.

---

## **8.2 The Pentagon, Bell Pottinger and Staged Psychological Warfare in Iraq**

---

Historically, the USG has had some success at carrying out PSYOP in favour of its aggressive military policies in Iraq. To gain support for the war in Iraq, the Joint Psychological Operations Task Force (JPOTF) worked to forge 'international support for the military effort in Northern Iraq... By conducting thoroughly planned and executed international information programs' (FAS, 2005, p.23). However, with the continued Iraqi insurgency that inflicted deaths on civilians and American troops, the US required an additional information campaign to shatter the ideological base and support for insurgent groups operating in Iraq.

Faced with the need to consolidate local support on the ground within Iraq, the USG sought the help of British PR firm Bell Pottinger. From 2007 to 2011, the USG spent over half-billion dollars on leveraging some of its PSYOP production to Bell Pottinger (Democracy Now, 2016). Well's participation in Bell Pottinger's propaganda operation in Iraq started in 2006 and finished in 2008. Bell Pottinger, much like North Korea during the 1950s capitalised on vivid images of death in a theatrical manner.

Well finessed videos that appeared to be crafted locally were crucial to US planners both in the Pentagon and US Generals on the ground in Iraq during the Second Gulf War. Wells's account of the propaganda themes was based on sensitive and prevalent occurrences such as a bomb exploding. According to Wells '[a] bomb would go off, a car bomb would go off, people would die, we'd have people out there filming it, it would come back we would then edit it into stories that would go out on various channels within the region' (The Bureau of Investigative Journalism, 2017). During the invasion of Iraq, car and suicide bombs were used as a tactic by insurgents. The US sought to win local support by portraying Al-Qaida in a violent and unfavourable light. Undoubtedly, the end goal was noble, but the means of achieving this was disingenuous. Bell Pottinger would edit videos in such a way to make it look:

*[A]s if it was made locally... It was more to make it look like it was Arabic, to make it look like it was shot in the region which it was ...To make it look like it was created by Arabic TV almost... It was given the impression that this was done by an Arabic company in my view (The Bureau of Investigative Journalism, 2017).*

Although, Bell Pottinger filmed atrocities that took place in Iraq, information concerning who filmed, edited and distributed such atrocities (in this particular scenario) was disguised to fulfil a purpose. That purpose was to mask the Anglo-American source that the content had derived from in order for the information to be received willingly by local Iraqi population who may have harboured anti-American sentiment due to the US occupation of Iraq. This would render Bell Pottinger's work as grey and potentially black propaganda, considering that the source of information was purposefully misconstrued.

Irrespective of whether the information or footage revealed is truthful or not, critics or adversaries of the US will be able to assert that the video was a form of propaganda

because it was one-sided. Al-Qaeda was not alone in killing Iraqi citizens. US airstrikes had killed many Iraqis, but footage of the aftermath of a failed US airstrikes did not follow after Bell Pottinger's product was aired in Iraq. The source of information is of great importance to those who observe information, because of the possibility that information is portrayed in a biased and incomplete manner.

Moreover, Bell Pottinger was also responsible for scripting soap opera-themed TV segments or television commercials which revolved around the notion that 'Al-Qaida are bad' and exonerated the positive outcome of people turning away from terrorism (The Bureau of Investigative Journalism, 2017; Fielding-Smith, Black and Ungood-Thomas, 2016). Reflexively, one would assume that turning away from reckless and pernicious bloodshed (terrorism) is the right decision to make. However, it is integral to acknowledge that explosions and bloodshed were symbolic messages being portrayed to Iraqi citizens and the international community.

To be specific, unrest in Iraq represented resentment to US occupation as well as America's failure to provide security to a foreign nation. The smaller the number of terrorist attacks that occurred, the greater the USG's ability was to claim that its occupation was a success. As crude as this point may come across, it was integral for Al-Qaeda to cause as much chaos as possible to bring light to America's inability to establish itself as a legitimate security provider in Iraq. US-inspired TV commercials that shunned terrorism served as a necessary ploy to reveal a specific narrative, much like the North Korean experience of staged propaganda.

Keeping Well's account in mind, it can be asserted that 'people seek security in direct relation to *who* they are' (Stern, 2006, p.187). By portraying a psychological other that is opposed to security and stability, the Pentagon attempted to accentuate its ontology by showing the world what they are not through propaganda videos. From one perspective '[t]he resort to propaganda may be a highly rational act' (Lasswell, 1935, p.188). From this angle, it can be claimed that Bell Pottinger's covert manipulation was necessary to steer the public against terrorists and to reduce America's concern that its ontology of being a benign state will endure the harsh local terrain.

Keeping in line with Mitzen conception of OS, states ‘need to bring uncertainty within tolerable limits, to feel confident that their environment will be predictably reproduced’ (2006, p.346). America’s confidence as a reliable security provider in Iraq is predicated on its ability to limit and reduce the impact of insurgent groups. From America’s standpoint, perhaps the democratic thing to do was to create propagandised videos, to ensure that local Iraqi’s are primed into making the correct choice in siding with democratic forces, over lawless insurgents. Despite the evolution from staged propaganda to modern TV commercials that are inspired and construed by foreign occupying nations, staging or selectively creating theatrical messages while masking the source of the content is a dangerous course of action to take. Nations that are caught concealing information in this particular context are often described as propagandists *with an agenda*.

Essentially, due to the extensive examples cited in chapter 3, the US has built up a significant amount of propaganda credit, or a reputation for engaging in propaganda, which would make it conceivable that they (US) would be willing to stage a form of psychological warfare. Should another flashpoint in global security concern a staged or highly orchestrated event, it would not be outlandish for a state to accuse the US of being responsible due to the vast history or propaganda credits that the US accumulated in the 20th and 21<sup>st</sup> century (see chapter 3 and 6). Orchestrating or staging theatrical propaganda leaves those who postulated the ruse open to counter propaganda claims that the accused is willing to make up events.

Clearly, there is a moral chasm between North Korea’s aforementioned staged propaganda and Bell Pottinger’s propaganda; however, the outcome of being exposed as a publicist or author of misleading information is similar. Global security providers such as the US require public trust and faith in their narratives in order to pacify dissent from disgruntled citizens, particularly in situations in which nations have agreed to host US military bases. In the case of Iraq, the US was not invited by Saddam Hussein, which ultimately makes the case of misleading the population far more amoral and problematic.

In addition to the theatrical propaganda that was created, Bell Pottinger tasked Wells with creating fake terrorist videos. According to Wells, his superiors had given him specific instructions to create fake terrorist propaganda that was predicated on Al-Qaeda footage. To be specific, Wells has asserted that his superiors made it clear to him that they wanted

him to make ‘this style of video and we’ve got to use al-Qaeda’s footage. We need it to be 10 minutes long and it needs to be in this file format and we need to encode it in this manner’ (The Bureau of Investigative Journalism, 2017). Well’s account highlights the heavily prosthetic and edited nature of their campaign. For this reason, the source of information will always be integral to know in case an unscrupulous organisation or rogue state is engaging in dirty tricks.

Moreover, to spread Bell Pottinger’s propaganda videos, the footage was saved on to a video compact disk (VCD) that was then purposefully dropped by US soldiers in houses during raids. Creating terrorist propaganda for consumption seems to be a running theme for the US in this thesis (see chapter 3, 4 and 6). The USG’s extensive experience in covert propaganda would suggest that although the US is a liberal democratic nation, it possesses a separate ontology that is antithetical to liberal values.

This assertion appears to be symmetrical with analysis cited in chapter 1 concerning the state and its multiple selves. Indeed, staging and editing the propaganda of an adversary appears to run contrary to what most US citizens assume their government is up to. Upon realisation that the alleged democratic leader of the free world is reproducing propaganda associated with terrorism, a great danger exists that the moral bar will be lowered. This may signal to other nations that creating covert propaganda is fair game (see chapter 6).

Despite the VCD format, the US had plans of tracking those who watched the propaganda video online via ‘google analytics’ (The Bureau of Investigative Journalism, 2017). In the view of Wells:

*These were disks that were made to play in...real player and what happened in real player is you’d get a white screen before anything would happen. They came up with this ingenious idea that within the white flash that real player does it actually tracks were the VCD is being played. Because real player has to connect online to run. That little bit of code would then be connected to a google analytics account so that way you could have a track and know where that VCD is being played (The Bureau of Investigative Journalism, 2017).*

In actuality, US propaganda was a surveillance scheme that attempted to track where its propaganda was being watched. At this juncture, readers can observe unequivocally that

at times, propaganda and surveillance are two sides of the same coin (see chapter 1). Well's went on to suggest that the analytics:

*Will tell you which IP address and where in the world it's being looked at... If one... shows up in another part of the world then that's the more interesting one. And that's what they're looking for more because then that gives you a trail of ok so someone sent it to this person or they've been here and they've gone elsewhere. So it gives you a track of someone who could possibly be a threat. Some of the VCD's ended up in some interesting countries, I think I had a couple in Iran... The most interesting one was in America. No idea how it got there (The Bureau of Investigative Journalism, 2017).*

This ingenious contraption enabled the US to keep an international tab on where its propaganda videos were being played to help verify who was passing material around (The Bureau of Investigative Journalism, 2017). At this stage of analysis, it seems that the familiar theme of US propaganda being at risk of contributing to what it is trying to fight has resurfaced. Or as put in Chapter 6, the democratic proselytisation of terrorism. I argue that America is so conditioned into being at conflict with other states and terrorists that the USIC is willing to produce covert propaganda to present a clear picture of an enemy that needs to be vanquished. However, when such endeavours are revealed to be false, US democracy becomes an emblem of hypocrisy and contributes to dangerous conspiracy theories that the US is *always watching and scheming*.

In Chapter 7, I argued that Soviet forgeries were based on believable narratives of US economic interest groups influencing America's foreign policy of global domination. This was particularly relevant in the Soviet Rockefeller letter. In the 21<sup>st</sup> century, the same phenomena can be repeated only this time concerning US theatrical propaganda in Iraq. Counter propaganda that accuses the US of a misdeed will be more believable as a result of America's past mistakes.

Portraying terrorists, as terrorists, is hardly a crime although democratic purists may look with disdain at covert psychological warfare. The option to bamboozle, seduce and cajole citizens into accepting a government constructed reality is part and parcel of democracy and to some extent the notion of governmentality (Lasswell, 1972, p.5; Dean, 2007, p.11).



However, as noted in Chapter 5 and 6, attempts to control OS can backfire and produce more risk. Undoubtedly, a running theme throughout this thesis is that great power nations which are attempting to placate their anxiety about the capricious environment they wish to shape and control, inadvertently produces offshoots of risk that challenges the original goal of alleviating OIS. Ironically, attempting to ‘manage the complexity of risk... give rise to new uncertainties’ (Beck, 2009, p.9).

Moreover, once covert propaganda is revealed to the public, an additional issue is created for the perpetrator. Post-revelation, adversaries have the opportunity to attribute conspiracies or half-truths, which now seem somewhat plausible due to the original sin of producing covert propaganda. In other words, the US has left its ontology open to multiple attacks from adversaries who may wish to tarnish the image of America irrespective of whether it has engaged in foul play or not. Bearing this in mind, it is vital to acknowledge that ‘[c]redibility is key to successful products because of the use and discovery of untruthful information irrevocably damages or destroys their and their originator’s credibility’ (FAS, 2005, p.124). In particular, the alleged 2018 chemical attack on Douma in Syria, which was blamed on Assad by the West, serves as a perfect example of why it is dangerous to create covert propaganda.

According to the BBC, ‘Syrian opposition activists, rescue workers and medics say more than 40 people were killed on 7 April in a suspected chemical attack on Douma’ (2018[c]). On the 9<sup>th</sup> of April, an emergency UN Security Council meeting was convened in which ‘France’s representative said thousands of videos and photos emerging from Douma in recent days showed victims foaming at the mouth and convulsing, all symptoms of a potent nerve agent combined with chlorine’ (UN, 2018[c]).

In direct opposition, Syria’s representatives noted that ‘[t]he White Helmets would fabricate evidence and Hollywood-like scenes intended to stir incitement against Syria and its allies’ (UN, 2018[c]). Here lies the problem. Due to the fact that in the past the US has created covert theatrical propaganda in Iraq, refuting claims that the West was behind the attack becomes difficult. In fact, on the 13<sup>th</sup> of April, Russian Foreign Minister Sergey Lavrov claimed to have “irrefutable evidence that it was another staging, and the special services of a state which is in the forefront of the Russophobic campaign had a hand in the staging” (Lavrov, 2018, cited in RT, 2018[c]).

Succinctly put, the West was staging chemical attacks in Syria, in the view of Lavrov. Similarly, during a Russian Ministry of Defense press briefing, General Igor Konashenkov, a spokesman for Russia's defence ministry has stated that “[w]e have... evidence that proves Britain was directly involved in organising this provocation” (Konashenkov, 2018 cited in BBC, 2018[d]). Knowledge of foul play, particularly from a government such as Britain and the US adds extra layers of suspicion concerning videos that circulate social media during times of war. Citizens at various levels of society are aware that intelligence services will go to great lengths to warp perception, as was the case with Bell Pottinger. No matter how outlandish the claim may be, so long as there is concrete evidence to prove that another democratic nation resorted to covert theatrical propaganda, individuals such as Lavrov can refute any responsibility for chemical attacks in Syria.

For those that are watching this spat take place, it becomes difficult to say for sure that any particular group or nation was responsible simply because, in recent memory, a democratic nation has created covert theatrical propaganda. Public opinion is, therefore, increasingly subject to the onset of OIS and confusion. Citizens around the world are faced with the two questions, what are Western governments up to in the Middle East? Who exactly are the terrorists? These questions are compounded further by the fact that conspiracy theories pushed by Russian state-owned news channel RT, revolve around the notion that the US-trained and created ISIS (RT,2014[a]; RT,2014[b]; RT,2017). America’s partnership with Bell Pottinger to create covert propaganda gives life to fringe elements on the Internet, and state figures such as Sergey Lavrov that have made accusations towards the West.

So long as there is credence to justify doubt in America’s integrity, conspiracy theories will be able to cite factual evidence, e.g. Wells’ account of Bell Pottinger’s work in Iraq, to back up outlandish, but now, not so outlandish claims. The citizen who is betwixt in this rather unusual situation in which bold claims have credence may end up losing faith in democratic adventures abroad even though no specific Syria based evidence was presented by Russia to suggest that America, Britain or a Western intelligence service was responsible for staging chemical attacks in Syria.

---

## 8.3 Conclusion

---

To conclude, a grave danger exists when sophisticated PR firms combine resources with intelligence services to produce theatrical propaganda. The question to contemplate at this stage is, what is stopping another non-state group from waging a similar campaign in ongoing conflicts? This only serves to incite and legitimise the actions of other nefarious actors who may see Western nations as hypocritical in their condemnation of propaganda. Ultimately, attempts by Western intelligence services to mitigate OIS in volatile terrains can go wrong and end up producing more risk that incites believable counter propaganda from adversaries. As pointed out by Martin, the VCD's somehow made it out of Iraq to the US, in which it is entirely plausible that if the VCD's garnered enough interest, someone could have created new copies and distributed them.

Once again, the US has taken the risky decision of devising ploys to track alleged terrorist while at the same time contributing towards the crystallisation of terrorist ideation and fascination. How then does the democratic leader of the free world explain to various nations that it knowingly placed propaganda material in the hands of potential terrorists? While this may have been an attempt to aggrandise America's visibility and knowledge of who the potential terrorists might be, it has left its ontological identity of a noble democrat at risk of being associated with amoral conduct that is usually reserved for Washington's enemies.

Moreover, the revelations made by Wells serves as an example of how non-state groups, at times, are nothing more than fodder for powerful states. So long as the price is right non-state groups may participate in morally questionable activities, which plays a contributory role in chipping away at the confidence of citizens to discern the truth from fiction in cyberspace. Bell Pottinger's actions are a reminder that Smith's DGC must focus significantly on non-state groups to limit the scope and means in which powerful states can manoeuvre and abuse their power. A key sticking point to conclude on is to ponder what power represents in this particular chapter. A running theme not only in this chapter but throughout this thesis concerns the means and the will to covertly shape perception. Power represents the right to deceive citizens, and if need be the citizens of other nations irrespective of the potential psychological reaction that propaganda may trigger. Power

represents the will of countries to uphold liberal values while part taking in secret intelligence operations. Ultimately, states have the near-impossible task of balancing how it fights in the shadows with democratic ideals and protecting their OS. In the long run, telling the truth is not such a bad idea.

---

## Chapter 9 Thesis Conclusion

---

Overall, I have come to the conclusion that nations have different selves which often clash. Nations, like individuals, have a sense of identity that often revolves around constructed ideals that are predicated on truth and fantasy. Western governments tend to perceive their sense of self as democratic, noble and benevolent. This sense of self is often in regular conflict with unsavoury acts and endeavours such as propaganda and surveillance, which are used to help nations survive an anarchic environment. How countries see and portray themselves determines how much leverage they have to do battle in the shadows against adversaries.

Throughout this thesis, it has been made clear that Western democratic states often struggle in the dark arts of dirty tricks not because they are inherently bad at propaganda and surveillance campaigns but because they are held to a higher moral standard than authoritarian regimes. Ultimately, a frictionless boundary between democratic veneers and an anarchic cyber environment is impossible to achieve. Pivoting from a place of democratic safety to the dark arts of covert propaganda is at times relatively simple for elite British and American intelligence services. On return to the original stance, states often experience OIS, particularly when they have been caught engaging in dirty tricks.

Moreover, this thesis has demonstrated emphatically that public opinion is betwixt in a battle of allegiance to various domestic and international actors. Citizens may not understand in entirety the extent to which intelligence services and non-state groups are trying to warp perception online. Nonetheless, it is too crude to assume that the public is a fumbling phantom. Chapter 5 shows that Russia's alleged information campaign against the US caused considerable OIS amongst Democratic Senators. Chapter 6 has revealed that US intelligence services act with an element of impunity in cyberspace to engage in deplorable propaganda and surveillance campaigns that are synonymous with entrapment.

No world power can stop the US from taking part in sowing black propaganda online. In fact, the US works alongside international partners to share intelligence derived from the fake sham universes that they have created. As such, cyberspace is in a state of anarchy paradoxically through inter-state cooperation, which has the potential to impact the OS of Internet users who are aware of leaked propaganda and surveillance measures in cyberspace.

In contrast to Chapter 5, chapter 7 indicates that the French had learnt from America's experience in the 2016 presidential election. Consequently, the experience of OIS amidst a tainted leaks campaign was not as practical as Russia's covert propaganda ploy in the US. Russia's alleged attempts of dirty tricks provided France with an example of how destructive modern cyber propaganda campaigns can be if the information and the overall campaign is not handled effectively. Although it is worth noting that the French and US examples are qualitatively different as the Russian leaks on Clinton contained real and embarrassing examples of how the DNC was ethically compromised. Unfortunately, people will continue to be deceived in cyberspace by propaganda campaigns. The FBI's democratic proselytisation of terrorism serves as a clear example that at times, the public indeed struggles to perceive reality in a way that Lippmann would not be surprised by. Indeed, the USG and Bell Pottinger's covert psychological warfare that was portrayed as legitimate news reifies the previous point that citizens may be unable to tell the difference between propaganda and truth.

Furthermore, chapter 8 has demonstrated that Western nations, such as the US are willing to engage in theatrical propaganda. The purpose of this chapter was to demonstrate that once a propaganda campaign of a nation is revealed, an adversary's nation is likely to capitalise on this occurrence and spin stories which accuse America or any other nation of engaging in staged propaganda. This is a detrimental process that chips away at the OS of the US and thus has the potential to limit American foreign policy due to a barrage of counter-propaganda campaigns that may be false but aligned to the real egregious sins of America's past. State attempts to mitigate OS within the field of propaganda in cyberspace has the potential to create further problems in the form of OIS.

This thesis aims to address the gap in knowledge concerning modern surveillance and propaganda methods, particularly those that were leaked by Snowden back in 2014 and

2015 (see chapter 1). Naturally, academics were attracted to mass surveillance programs such as Prism and Tempora. However, very little was written about GCHQ's subunit JTRIG, which employed both surveillance and propaganda techniques to influence perception in cyberspace. However, even when this did feature in Bakir's work, very little was written to develop on this niche area by other academics. In a post-2016 US presidential election world where JTRIG's playbook was emulated to influence the US public opinion, it is vital that this area be thoroughly assessed. Although I have demonstrated that the CIA and other agencies previously enacted some of JTRIG's manoeuvres in the physical world, this research aimed to assess the relatively new platform of cyberspace.

To be precise, the purpose of this extensive research was to bring together international examples of modern propaganda and surveillance measures that resemble JTRIG's efforts to sway perception in foreign countries, and scrutinise how this can have a detrimental impact on OS at the state and individual level. With respects to OIS, the aims and objective of this study was to demonstrate that attempts by states to mitigate OIS, can heighten state anxiety once high-risk manoeuvres have backfired or been exposed. This objective was met in the analysis of chapter 5, 6 and briefly in 8.

Furthermore, this thesis aimed to assess whether or not, it is reasonable to refer to the public as a phantom public that is ill-equipped to deal with sophisticated or rudimentary cyber propaganda manoeuvres postulated by intelligence services and non-state groups. This, again, was addressed in chapter 7. Moreover, an additional objective was to assess the impact that such clandestine measures can have on public opinion. Would the public be susceptible to experiencing OIS or be sufficiently informed to endure propaganda ploys by intelligence services? This thesis demonstrated that the phantom public is a pejorative term that cannot unequivocally be applied to the modern 21<sup>st</sup> century since France was not rocked by the presidential tainted leaks campaign aimed at President Macron.

Additionally, this thesis has demonstrated beyond unreasonable doubt that intelligence services continue to work tirelessly to undermine or be prepared to undermine OS and cybersecurity. OS is thus no longer a concept that is bound to sociology but applicable to various other fields, including IR and Security Studies (propaganda and surveillance).

Much to the dismay of privacy advocates, the anarchic system that democracy inhabits compels intelligence services to cut loose and drop the democratic anchor in the ocean, to save the very model of governance (democracy) that forbids or frowns at unsavoury acts. The only problem is navigating back to the original point in which the anchor was set loose. States may find it tempting to use dirty tricks regularly in the face of so-called democratic values.

Therefore, propaganda will continue to be a useful tool for democratic nations to wield against adversaries throughout the world. Explaining the necessity of propaganda and surveillance in a democratic way may prove to be a significant challenge. It is entirely possible that if a cultural shift is adopted, which includes explaining the need to use black propaganda, democratic purists will experience more OIS. Avoiding the topic altogether is equally problematic as citizens are more susceptible to believing the democratic veneer which shields sight of Western dirty tricks in cyberspace. When leaks are exposed, the cycle starts all over again. Therefore, OIS is an inescapable factor for democracies and society in general.

The anarchic environment that intelligence services and citizens operate in needs an intermediary force to help mitigate propaganda and surveillance campaigns. As covered in Chapter 3, non-state intermediaries or a DGC is greatly needed. However, I do not see this as a plausible or realistic option that will alleviate or extirpate tainted leaks or the FBI's NTNI. States often react out of fear and permit their intelligence services to undermine the security of other citizens and nations. As I see things, this will be an endless struggle in cyberspace, until technology renders the efforts of states and non-states completely useless.

Perhaps a cataclysmic event concerning cybersecurity will force all states into a compromise. While Realism has come under scrutiny by many critics for being an obsolete theory, in cyberspace, Realism is a relevant and credible paradigm that can help to explain the current state of affairs. Indeed, I do accept that Kaspersky, Trend Micro, FireEye and other cybersecurity vendors play a key role in bolstering network security. This admission would suggest Liberalism is a crucial theory. However, the gravitational pull of anarchy and offensive Realism is too great to believe that at present, states will

cease hostilities and the use of dirty tricks because of a DGC and notions of cyber stability.

---

## 9.1 Contribution to Knowledge

---

Overall, this thesis makes several contributions to academic knowledge. Firstly, my thesis has attempted to develop an understanding and knowledge concerning JTRIG's activity in conjunction with comparing it (JTRIG) to recent examples of propaganda and surveillance measures. Moreover, my research contributes to new knowledge since my thesis addresses Snowden leaks that were not researched thoroughly by an extensive amount of academics. By this, I am referring to specific tactics outlined by JTRIG, which were being used by other intelligence services and non-state groups (see chapter 1, 2, 3, 4 and 5).

Specifically, this research aims to demonstrate that attempts by states to mitigate OIS, can have a counterproductive effect in a Realist environment that pushes competitive nations into engaging in morally questionable acts. As a result of interstate competition in cyberspace, the experience of OIS is becoming a regular theme. This particular objective is addressed in Chapter 6 and 8. In chapter 6 and 8, the USG attempted to curtail the level of OIS by engaging in propaganda and surveillance methods to sway the perception of potential and actual terrorist sympathisers. As a consequence of dealing with probabilities, the USG ended up crystallising terrorist ideation of individuals that may have decided to turn away from terrorism if a de-radicalisation intervention program was applied. Post-revelation of the USG's online operations, it is challenging to associate US narratives with the truth much to the delight of America's adversaries that push anti-American propaganda.

This was a particularly controversial issue in 2018 as Russian state representatives accused Western intelligence services of staging chemical attacks in Syria. Because the Pentagon was caught using British PR firm Bell Pottinger to edit and create theatrical propaganda, the former accusation is thus an issue for America's identity in different parts



of the world. In other words, modern attempts by the USG to shape the information environment often ends up increasing what it fears – that is, a loss of influence.

Additionally, Chapter 6 has contributed to academic knowledge by looking at how the FBI created online environments that flirt with the concept of entrapment. In this example, I demonstrated that the FBI's online presence could lead to a situation in which Internet communications amongst citizens takes place within a sham universe. Post revelations of this scheme, OIS among Internet users can become a persistent feature of the Internet.

An additional objective was to verify whether or not it is reasonable to refer to the public as a phantom public that is ill-equipped to deal with sophisticated or rudimentary cyber propaganda manoeuvres postulated by intelligence services and non-state groups. This thesis contributes to knowledge since there is not a significant amount of academics that have tackled such a sensitive question in conjunction with modern propaganda and surveillance activities. By employing the writings of Lippmann and juxtaposing it with the case study 3, I was able to demonstrate instances in which a phantom public may become relevant as a concept. However, ultimately I demonstrated that it is somewhat myopic to generalise or apply the term phantom public to all of society. Indeed, it may be tempting for some commentators to criticise the average citizen and bring his/her intelligence into question. Conversely, a phantom is too strong of a word to associate with an entire country.

In consideration of the fact that this research provides the theoretical foundations for future researchers to analyse this field, my analysis holds significance in the area of propaganda and surveillance. This is not to imply that the aforementioned body of work is impeccable but rather to highlight the necessity of its presence due to the gap in knowledge. As will be discussed in the cross-chapter section, improvements can be made with which future researchers can take the reins and develop. Furthermore, my research is of significance to the field of propaganda and surveillance because it has demonstrated that OS is a significant theory that can be used to evaluate JTRIG's playbook of covert dirty tricks. My research justifies why OS should be welcomed into the lexicon of IR. In Chapter 5, OIS was displayed by 3 Democratic Senators. Chapter 5 portrays three Democratic Senators that are desperately trying to protect America's sense of self during and after the US 2016 presidential election. Additionally, my research has combined both

propaganda and surveillance while successfully demonstrating that propaganda and surveillance are two sides of the same coin.

---

## 9.2 Cross Case Study Reflections

### 9.3 Chapter 5

---

Chapter 5 provided the most significant analysis of OIS. This particular case study is predicated on the unresolved case of the 2016 US presidential election and Russia's alleged involvement in hacking and releasing information. Understandably, it is still difficult to make concrete judgments concerning who was responsible. Having said this, what is evident from this case study is that white propaganda, which is truthful information that is released with an agenda, is at times more powerful than years of secreting covert black propaganda. As demonstrated in Chapter 3, the CIA, on various occasions, made use of black propaganda. Conversely, America's sense of OS was rocked by a mixture of Russian based white, grey and black propaganda during the US 2016 presidential election. States have become hypersensitive to the methodology of hack and release of information with countries such France and the UK have called into question whether Russia has been trying to interfere or influence their democratic process (Garraway and Smith, 2017; Rose and Dyomkin, 2017).

This hypersensitivity is a direct result of witnessing the world's superpower become so divided in such a toxic manner in a short space of time. OS is thus something that needs to emerge from the shadows of physical security and become a credible point of reference in IR scholarship and research areas that focus on cyberspace. Evidence cited in this chapter demonstrates the distress and fear that various Senators were projecting. Prominent themes elicited from the three Senators revolved around America's lack of agency to react appropriately in light of its lack of unity on the matter. Furthermore, US Democratic Senators were concerned about future attacks and similar campaigns waged by adversaries. Iranian propaganda is an example of Congressman Warner's nightmare beginning to manifest (FireEye, 2018).

Moreover, Senator Warner, in particular, inadvertently summed up the issue that the world faces today. Concerned about Russia's playbook being used by foreign adversaries,

Senator Warner failed to mention America's vast propaganda history. Failure to apply a reasonable standard between the West and its foreign adversaries is the crux of the continuation of Realist anarchy and discourse. One of my main objectives concerning how I will write this thesis was to provide a body of knowledge that counters the contemporary obsession with Russian dirty tricks.

In reflection, both Western allies (UK and USA) and Russia are in a constant battle of influence, which requires high-risk activity in cyberspace to conquer the other. An exciting angle for future researchers to take is to investigate if Russia fears other nations making use of the playbook that Senator Warner spoke of. Is Russia ontologically secure enough to withstand a tainted leaks type scandal that showed Putin in an incredibly unfavourable light amongst the Russian citizens? Perhaps in the aftermath of this study, researchers can investigate the extent to which patriotism affects OS amidst state-wide scandals.

---

## 9.4 Chapter 6

---

Throughout this body of work, it has become clear that states often react out of fear of foreign adversaries and their domestic advocates. Also, it has become apparent that states are willing to go to great lengths to reduce the amount of risk they are exposed to in cyberspace. Cyberspace offers states an arena to launch propaganda and surveillance campaigns without being unequivocally caught in the act. Propaganda and surveillance campaigns that are used to curtail perceived threats often end up producing new risks. In the case of the FBI's democratic proselytisation of terrorism, cyber sting operations may have been originally viewed as an ingenious ploy to attract people who might be radicalised beyond the point of no return. Attracting hardened terrorist sympathisers and extracting evidence may also appear like a successful scheme that is keeping the homeland safe.

However, as pointed out in Chapter 6, this particular case study was more complicated than attracting hardened terrorist to a website and collecting evidence without incitement. To keep up the sham universe, the FBI had to play the role of a terrorist organisation by claiming to be able to provide training, route planning and bus tickets for Tounisi.

Knowledge of this, in many respects, contributes to the idea that Muslims are being targeted. As previously noted by Patel in Chapter 4, surveillance in white-majority societies tend to focus on brown bodies from South Asia and the Middle East (2012, p.230). As a direct consequence of the FBI's actions, Patel's suggestion has been qualified, to an extent. To say the least, Western democratic values have been tarnished, paradoxically, in the name of protecting democracy. Perhaps Taylor was correct in citing the democratic myth which revolves around the notion that everyone else but democracies engage in propaganda (2002, p.437).

The point to be made here is that for some time, democratic states have struggled to walk on a straight and narrow path designed purely for democracies. To a great extent, democracies are fixated with promoting human rights worldwide, up until they directly or indirectly end up violating article 20 of the International Covenant on Civil and Political Rights that prohibits war propaganda (OHCHR, 2019[a]). Often Western intelligence services veer off course and end up sacrificing the human rights of some in order to protect the human rights of other groups. The inability of the USIC to collect intelligence on Muslims online in a purely democratic manner if such a thing exists is the product of a long history of questionable covert intelligence operations.

Furthermore, upon reflection of Chapter 6, a great danger exists concerning the FBI's covert joint operations with international partners (FBI, 2015, p.17). This opens up online platforms to more possibilities and risks, which if left unchecked, can lead to multiple sham universes being created across the world in the name of security. What kind of future will the international community be left with if the FBI spreads this methodology of quasi or actual entrapment abroad to allies that have less care for democratic standards? Cyberspace is thus going to experience some of the most ingenious yet controversial intelligence operations that destroys the chance of establishing a DGC.

Overall, in a post-9/11 world where America's physical and OS was challenged, acting out of fear to preserve the self both physically and ontologically has ironically attracted detrimental drawbacks. The question for academics at this stage is, how are intelligence services supposed to reduce or end cyber propaganda and surveillance practices that contravene democratic principles? Also, the Muslim community may fall victim again to clandestine measures. In order for insight to be developed, future researchers should

conduct semi-structured interviews with Muslim communities in the US to find out whether such revelations in Chapter 6 will have an impact on their Internet activity or perception of self when operating in cyberspace. Lastly, it is also essential to explore the dangers of non-state groups that may create fictional propaganda websites in foreign countries for the sake of forging a sham universe to match their social beliefs about Muslims or any other group. In other words, what is stopping a group of Islamophobic individuals from replicating the FBI's methodology? This indeed is an area that needs to be explored.

---

## 9.5 Chapter 7

---

Within this chapter, it became self-evident that tainted leaks can encourage a spiral of doubt and a lack of trust in information irrespective of whether this is fleeting or a long term issue. Specifically, it also became evident that at times people may struggle to perceive the invisible hand that is pulling the strings of public opinion. Society is at risk of sliding into a heavily edited reality that is predicated on the process of hacking – editing and releasing information. As expressed in Chapter 7, the concept of the phantom public is a poignant but an over-exaggeration of how incapable the average citizen is at dealing with domestic affairs such as spotting propaganda. In the case of the US 2016 presidential election, the phantom public would have a stronger case due to the long-term societal division that has been caused.

The 2017 French presidential elections served as an example that tainted leaks can have a limited impact on societal perception. Tainted leaks as a technique of propaganda may resurface again in the future, but if it is to be successful leaks would need to appear more authentic. This places a great burden on organisations such as the Citizens Lab to help counter-propaganda ploys. Ironically, this is a clear example of how liberal institutions have a role to play within IR.

On the other hand, in the case of tainted leaks, society is yet to see a sophisticated dirty tricks campaign that has caused more damage than the US 2016 election (propaganda). The closest example that has emerged is the email release concerning Qatar's support for Iran, which sent shockwaves through the Gulf. Regardless, this example demonstrates

that public opinion is in danger, although not quite to the extent to which society has been relegated to a phantom. Although Cold War groups such as the KGU carried out similar roles in East Germany, the example of tainted leaks differs in the fact that the modern cyber era paves the way for the debauchery on a grand scale. As technology develops, non-state groups may devise a way to make forgeries appear incredibly authentic.

---

## 9.6 Chapter 8

---

Upon reflection, it appears that non-state groups or institutions need to be greatly scrutinised. Bell Pottinger's role in the Pentagon's plan to create theatrical propaganda in Iraq emphasises the danger that non-state groups find themselves in when large sums of money are presented to them for their services. Ultimately the onus is on the company. However, Chapter 8 highlights the international reach of propaganda campaigns. What is remarkable from such an endeavour by the Pentagon was the production of VCD's which contained Bell Pottinger's theatrical propaganda. Once an individual watched this video online, the US was able to track where it was being watched. At times it is misleading to speak of propaganda and surveillance as two completely separate fields. Without surveillance, many propaganda endeavours are not as potent.

Furthermore, this chapter emphasises the reality of a Realist cyber anarchic environment that states operate within to compete with adversaries. Although the use of a non-state institution like Bell Pottinger would indicate that state power and rivalry can be significantly influenced by non-state groups, the point to take from this case study is that states find themselves physically and ontologically under pressure to push critical narratives in times of war. From an ontological perspective, America needed to tell its story within Iraq; a nation that was hostile to the presence of US troops.

Furthermore, storytelling is an incredibly powerful tool for the US to wield as a means of convincing its domestic population that they were righteous in their endeavour to fight terrorism in Iraq. However, this aim becomes lost when it is revealed that the democratic leader of the free world has promulgated scripted theatrical propaganda in the name of democracy. At this juncture, the US is unable to convincingly push narratives without impediment by adversaries that remind the world of the vast history and contemporary

examples of US foreign propaganda campaigns that I have highlighted throughout this thesis.

---

## 9.7 Limitations of the Study

---

While this thesis has proficiently dissected multiple areas that contribute to academic knowledge, I have identified three predominant weaknesses. Firstly, my methodology is based on document analysis and online research. To some, this may be a significant cause of concern as it limits my ability to test a theory or narrative with participants in order to gauge societal responses to a particular inquiry. Moreover, with regards to quantitative measures of inquiry, it will be difficult to generalise any form of discussion points. Secondly, this research focus is based on an area that is difficult to study. Propaganda and surveillance revelations are predicated mainly on leaks, which do not happen as regularly as researchers would like. Top Secret documents concerning propaganda and surveillance campaigns are heavily guarded secrets within governments.

Leaking Top Secret information comes with a considerable amount of risk to whistle-blowers, which in many respects, deters the flow of information. In other words, due to the drastically curtailed information flow that comes from intelligence services or whistle-blowers to the population, it is hard to know exactly what is happening within intelligence services. In reality, interested researchers operate off of snapshots that are based on a specific time in the past. Since the Snowden leaks, GCHQ may have created new units that are far more aggressive than JTRIG was in the past.

Moreover, GCHQ may have altered their focus and begun targeting different areas that I have not covered. Dependency on whistle-blowers is thus a potential roadblock to the development of knowledge. It would, therefore, be quite challenging to build upon this thesis. Having said this, leaks in the cyber age have become relatively common.

---

## 9.8 Final Remarks

---

Propaganda and surveillance campaigns will continue to erode the confidence of Internet users as nations wage influence operations around the world. The addition of non-state groups to the equation has compounded the issue further to the extent that more

WikiLeaks type groups may manifest themselves in the future and hold nations over a barrel. The US 2016 presidential elections served as an excellent example to demonstrate how startled politicians can be with regards to Russia's alleged propaganda and surveillance campaign. If the average individual discovered that this playbook was being used in such a dystopian way on a regular basis, society would be overwhelmed with risk.

However, if JTRIG's playbook and theatrical propaganda are becoming standard practice by the US and foreign intelligence services, perhaps the sham universe will be the new norm. Considering the history of the OSS's Morale Operations in WW2, the IRD's grey and black propaganda in Nigeria and Latin America, the FBI's COINTELPRO anonymous letter campaign, and the CIA's black propaganda in Latin America that was cited in Chapter 3; perhaps it is inevitable that cyberspace will become a cesspool of well-crafted lies. Indeed, it may have been naïve of society to assume that the standard set in the physical world would dramatically change in the realm of cyberspace for the greater good of humankind. OIS may become a prominent feature of cyberspace since nations will not relinquish offensive Realist impulses.

Moreover, in between international attempts to sway perception by multiple governments are citizens that struggle to verify the integrity of information. It does not appear that propaganda operations will cease. Therefore, it is vital that independent organisations continue to fact check information. Organisations such as Citizens Lab have done a great job studying the technical means of surveillance and propaganda operations such as tainted leaks. However, considering the voluminous nature of the Internet, this may prove to be a difficult task. Perhaps society must adapt to JTRIG's playbook by being far more independent thinkers as opposed to depending wholeheartedly on government narratives. Such a move may appear to be ideal for foreign propagandists considering how exposed people are to the cacophony of narratives in cyberspace. Having come full circle, this conundrum does not appear resolvable in the near future.

In my opinion, it would take a cataclysmic phenomenon to force states to the negotiation table or for technology to render such propaganda and surveillance measures inadequate. Until states and non-state groups force a cosmopolitan DGC into existence, society must cope with the deluge of claims and counterclaims that are generated and pushed online by an invisible or near-invisible hand. In many ways, this thesis acts as a manual for how



states have over time developed and made use of both propaganda and surveillance to further state goals. This thesis highlights the effects of OIS at the state level and broader society due to propaganda and surveillance campaigns. Ultimately, propaganda and surveillance are potent weapons in cyberspace that need to be regulated to save future generations from being subjected to egregious lies that may change the course of human history for the worse.

---

## Reference List

---

- Ackerman, S. and Ball, J. (2014) *Optic Nerve: millions of Yahoo webcam images intercepted by GCHQ*. Available at: <https://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo> (Accessed: 1 May 2017).
- African Wildlife Foundation (n.d.) *Our Mission*. Available at: <https://www.awf.org/> (Accessed: 11 November 2018).
- Agee, P. (1975) *Inside the Company: CIA Diary*. New York: Stonehill Publishing Company.
- Agee, P. (1978) 'Where Do We Go From Here' in Agee, P. and Wolf, L. (ed.) *Dirty Work. The CIA in Western Europe*. New York: Dorset Press, pp. 250 – 285.
- Agius, C. (2016) 'Drawing the discourses of ontological security: Immigration and identity in the Danish and Swedish cartoon crises', *Cooperation and Conflict*, 52(1), pp. 109-125.
- Aldrich, R.J. (2011) *GCHQ The Uncensored Story of Britain's Most Secret Intelligence Agency*. London: HarperPress.
- Aljazeera (2018) *Full text of John Bolton's speech to the Federalist Society*. Available at: <https://www.aljazeera.com/news/2018/09/full-text-john-bolton-speech-federalist-society-180910172828633.html> (Accessed: 20 November 2018).
- American Civil Liberties Union (2012) *Italian Court Upholds Rendition Conviction of CIA Agents*. Available at: <https://www.aclu.org/blog/national-security/torture/italian-court-upholds-rendition-conviction-cia-agents> (Accessed: 3 November 2019)
- Amnesty International (2009[a]) African Union refuses to cooperate with Bashir arrest warrant. Available at: <https://www.amnesty.org/en/latest/news/2009/07/african-union-refuses-cooperate-bashir-arrest-warrant-20090706/> (Accessed: 1 January 2020)

Amnesty International (2009[b]) *US deadly drone strikes*. Available at:

<https://www.amnesty.org.uk/thank-you-us-deadly-drones> (Accessed: 14 December 2019)

Amnesty International, (2018) *What are human rights?* Available at:

<https://www.amnesty.org.uk/what-are-human-rights> (Accessed: 30 November 2019)

Anderson, D. (2016) *Report of the Bulk Powers Review*. (Cm 9326). Available at:

<https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2016/08/Bulk-Powers-Review-final-report.pdf> (Accessed: 25 December 2017).

Andregg, M.M. and Gill, P. (2014) ‘Comparing the democratization of intelligence’, *Intelligence and National Security*, 29(4), pp.487-497.

Andrew, C (n.d.) *The British Empire and Commonwealth*. Available at:

<https://www.mi5.gov.uk/the-british-empire-and-commonwealth> (26 April 2020)

Andrew, C. (2010) *The Defence of the Realm: The Authorized History of MI5*. London: Penguin.

Andrew, C. (2018) *MI5 in World War 1*. Available at: <https://www.mi5.gov.uk/mi5-in-world-war-i> (Accessed: 25 April 2018).

AnonHQ, (2014) *Anonymous Revealing Ku Klux Klan’s Identities – Operation #OpKKK*.

Available at: <https://anonhq.com/anon-reveals-klk-identities-opkkk/> (Accessed 1 July 2015).

Arab Forum for Environment and Development (2018) *Mission Statement*. Available at:

<http://www.afedonline.org/en/inner.aspx?menuID=4> (Accessed: 11 November 2018).

Anyadike, O. (2016) *Exclusive: Top UN Whistleblower Resigns, Citing Impunity and Lack of Accountability*. Available at:

<https://www.thenewhumanitarian.org/news/2016/06/07/exclusive-top-un-whistleblower-resigns-citing-impunity-and-lack-accountability> (Accessed: 9 May 2016).

Associated Press (2016) *Sen. Warren '100%' Concerned With Russia Hacking*. Available at:

<https://www.youtube.com/watch?v=sxpdofUix9Y> (Accessed: 25 May 2018).

'A Symposium on Intelligence Ethics' (2009) *Intelligence and National Security*, 24(3), pp. 366-386.

Asian Environmental Society (2018) *Asian Environmental Society (AES)*. Available at:

<https://uia.org/s/or/en/1100037294/> (Accessed: 11 November 2018).

Auchard, E. (2018) *Macron Campaign Was Target of Cyber Attacks by Spy-Linked Group*.

Available at: <https://uk.reuters.com/article/us-france-election-macron-cyber/macron-campaign-was-target-of-cyber-attacks-by-spy-linked-group-idUKKBN17Q200> (Accessed: 7 July 2018).

Australian War Memorial (n.d.) *China (Boxer Rebellion), 1900–01*. Available at:

<https://www.awm.gov.au/articles/atwar/boxer> (Accessed: 16 December 2018).

Australian War Memorial (2020) *Malayan Emergency*. Available at:

<https://www.awm.gov.au/articles/atwar/malayan-emergency> (Accessed: 25 April 2020)

Bailey, K.D. (1994) *Methods of Social Research*. 4<sup>th</sup> edn. New York: The Free Press.

Baines, P.R. and O'Shaughnessy, N.J. (2014) 'Political Marketing and Propaganda: Uses, Abuses, Misuses', *Journal of Political Marketing*, 13(3), pp. 1-18.

- Bakir, V. (2015[a]) 'News, Agenda Building, and Intelligence Agencies A Systematic Review of the Field from the Discipline of Journalism, Media, and Communications', *The International Journal of Press/Politics*, 20(2), pp. 131-144.
- Bakir, V. (2015[b]) "'Veillant panoptic assemblage": Mutual watching and resistance to mass surveillance after Snowden', *Media and Communication*, 3(3), pp.12-25.
- Bamat, J. (2015) *Voltaire 'tolerance' book flies off shelves after Paris attacks*. Available at: <https://www.france24.com/en/20150114-france-charlie-hebdo-voltaire-book-best-seller-treatise-tolerance> (Accessed: 11 May 2019).
- Bayly, M.J. (2015) 'Imperial ontological (in) security: 'Buffer states', International Relations and the case of Anglo-Afghan relations, 1808–1878', *European Journal of International Relations*, 21(4), pp. 816-840.
- BBC, (n.d.) *Slavery - a timeline*. Available at: [http://www.bbc.co.uk/liverpool/localhistory/journey/american\\_connection/slavery/timeline.shtml](http://www.bbc.co.uk/liverpool/localhistory/journey/american_connection/slavery/timeline.shtml) (Accessed: 1 November 2019)
- BBC (2012) *Ethiopia to host Africa Union summit after Omar al-Bashir Malawi row*. Available at: <https://www.bbc.co.uk/news/world-africa-18407396> (Accessed: 1 January 2020)
- BBC (2014) *Kitchener: The Most Famous Pointing Finger*. Available at: <http://www.bbc.co.uk/news/magazine-28642846> (Accessed: 15 May 2018).
- BBC (2015[a]) *Frogman Files Show Blunders Surrounding Cdr 'Buster' Crabb's Death*. Available at: <https://www.bbc.co.uk/news/uk-england-34605107> (Accessed: 5th July 2018).
- BBC (2015[b]) *Paris attacks: What happened on the night*. Available at: <https://www.bbc.co.uk/news/world-europe-34818994> (Accessed: 25 April 2019).

- BBC (2016[a]) *EU referendum: Baroness Warsi switches from Leave to Remain*. Available at: <https://www.bbc.co.uk/news/uk-politics-eu-referendum-36572894> (Accessed: 7 December 2019)
- BBC (2016[b]) *Paris attacks: Call to overhaul French intelligence services*. Available at: <https://www.bbc.co.uk/news/world-europe-36711604> (Accessed: 1 March 2019).
- BBC (2017[a]) *How BAE sold cyber-surveillance tools to Arab states*. Available at: <http://www.bbc.co.uk/news/world-middle-east-40276568> (Accessed: 10 November 2017).
- BBC (2017[b]) *South Korea's spy agency admits trying to influence 2012 poll*. Available at: <http://www.bbc.co.uk/news/world-asia-40824793> (Accessed: 21 February 2018).
- BBC (2017[c]) *IS foreign fighters: 5,600 have returned home – report*. Available at: <https://www.bbc.co.uk/news/world-middle-east-41734069> (Accessed: 2 March 2019).
- (BBC, 2018[a]) *Germany starts enforcing hate speech law*. Available at: <https://www.bbc.co.uk/news/technology-42510868> (Accessed: 8 December 2019)
- BBC (2018[b]) *Trump sides with Russia against FBI at Helsinki summit*. Available at: <https://www.bbc.co.uk/news/world-europe-44852812> Accessed: 19 February 2019.
- BBC (2018[c]) *Syria war: What we know about Douma 'chemical attack'*. Available at: <https://www.bbc.co.uk/news/world-middle-east-43697084> (Accessed: 10 July 2018).
- BBC (2018[d]) *Russia says Syrian 'chemical attack' was staged*. Available at: <https://www.bbc.co.uk/news/world-middle-east-43747922> (Accessed: 12 June 2018).
- (BBC, 2019[a]) *MI5's use of personal data was 'unlawful', says watchdog*. Available at: <https://www.bbc.co.uk/news/uk-48597111> (Accessed: 3 November 2019)

BBC (2019[b]) *Data leak reveals how China 'brainwashes' Uighurs in prison camps*. Available at: <https://www.bbc.co.uk/news/world-asia-china-50511063> (Accessed: 2 November 2019)

BBC, (2019[c]) *Blood Sunday: Man shot in chest awarded compensation*. Available at: <https://www.bbc.co.uk/news/uk-northern-ireland-foyle-west-5059216> (Accessed: 30 November 2019)

BBC, (2019[d]) *Paris climate accords: US notifies UN of intention to withdraw*. Available at: <https://www.bbc.co.uk/news/world-us-canada-50297029> (Accessed: 19 December 2019) (ctrl F Paris accord's)

BBC Radio 4 Today (2019) *Should intelligence agents be able to commit crimes in certain circumstances? The govt and MI5 today face a legal challenge to clarify when and what crimes can be committed. MI5's ex-director general, Lord Jonathan Evans, explains why such rules exist #r4Today @MishalHusain* [Twitter] 5 November. Available at: <https://twitter.com/bbcr4today/status/1191663054968283137?s=12> (Accessed: 11 December 2019)

Beaglehole, E., B. A. (1928) 'Some aspects of propaganda', *The Australasian Journal of Psychology and Philosophy*, 6(2), pp.93-110.

Beck, U. (2006) 'Living in the world risk society', *Economy and Society*, 35(3), pp. 329-345.

Beck, U. (2009) 'Critical theory of world risk society: a cosmopolitan vision', *Constellations*, 16(1), pp. 3-22.

Beck, U. (2016) *The Metamorphosis of the World*. Cambridge: Polity Press.

Bedfordshire Police (2019) *What is Cyber Crime?* Available at: <https://www.bedfordshire.police.uk/information-and-services/Crime/Cyber-crime-and-online-safety/What-is-cyber-crime> (Accessed: 30 November 2019)

- Bellaby, R. (2012) 'What's the Harm? The Ethics of Intelligence Collection', *Intelligence and National Security*, 27(1), pp. 93-117.
- Bennet, G. (2016) *What's the Context? 9 May 1956: Eden orders an enquiry into the disappearance of Commander 'Buster' Crabb*. Available at: <https://history.blog.gov.uk/2016/05/09/whats-the-context-9-may-1956-eden-orders-an-enquiry-into-the-disappearance-of-commander-buster-crabb/> (Accessed: 5 July 2018).
- Berg, N. (2008) 'Joseph Wulf: A Forgotten Outsider Among Holocaust Scholars' in Bankier, D and Michman, D (ed.) *Holocaust Historiography in Context: Emergence, Challenges, Polemics and Achievements*. Jerusalem: Yad Vashem, pp. 167-206.
- Berry, D. (2011) 'The Computational Turn: Thinking about the digital humanities', *Culture Machine*, 12, pp.1-21.
- Bernal, P. (2016) 'Data gathering, surveillance and human rights: recasting the debate', *Journal of Cyber Policy*, 1(2), pp.243-264.
- Bernays, E. (2005) *Propaganda*. Rev. edn. New York: Ig Publishing.
- Biddle, W.W. (1931) 'A psychological definition of propaganda', *The Journal of Abnormal and Social Psychology*, 26(3), pp.283 – 295.
- Big Brother Watch and Others v. The United Kingdom (2018). European Court of Human Rights. Application no. 58170/13, 62322/14 and 24960/15 [Online]. Available at: <https://hudoc.echr.coe.int/eng#%7B%22itemid%22:%5B%22001-186048%22%5D%7D> (Accessed: 3 November 2019)
- Biles, P. (2012) *Falklands invasion 'surprised' Thatcher*. Available at: <https://www.bbc.co.uk/news/uk-20800447> (Accessed: 22 April 2020)



Bimfort, M. T (2011) *A Definition of Intelligence*. Available at:

[https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol2no4/html/v02i4a08p\\_0001.htm](https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol2no4/html/v02i4a08p_0001.htm) (Accessed: 22 December 2018).

Bird, J. and Bird. J. (2013) *Penetrating the Iron Curtain: Resolving the Missile Gap with*

*Technology*. Available at: <https://www.cia.gov/library/publications/cold-war/resolving-the-missile-gap-with-technology/missile-gap.pdf> (Accessed: 2 December 2019)

Blake, A. (2019) *John Kennedy vs. Vladimir Putin: How Trump defenders' Ukraine talking points compare to what Russians say*. Available at:

<https://www.washingtonpost.com/politics/2019/12/02/sen-john-kennedy-gop-alliance-with-russian-propaganda/> (Accessed: December 10 2019)

Blanton, S.L. and Kegley, C.W. (2017) *World Politics Trend & Transformation*. Boston: Cengage Learning.

Bloomberg Politics (2018) *Sen. Warren Says Trump 'Sucking Up' to Putin*. Available at:

<https://www.youtube.com/watch?v=wofALGTuKvg> (Accessed: 19 February 2019).

Blum, W. (1986) *The CIA a forgotten history*. London: Zed Books Ltd.

Blum, W. (2003) *Killing Hope U.S. Military and CIA Interventions Since World War I*. London: Zed Books.

Blumer, H. (1969) *Symbolic Interactionism: Perspective and Method*. Berkeley: University of California Press.

Boghardt. T. (2015) *The Fighting Group against Inhumanity: Resistance and Espionage in the Cold War, 1948–1959*. Available at: <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol-59-no-4/pdfs/Boghardt-The-Fighting-Group.pdf> (Accessed: 10 November 2017).

- Bond, D. (2018) *MPs criticise tech groups and UK government over terror attacks*. Available at: <https://www.ft.com/content/11d863e0-ee30-11e8-89c8-d36339d835c0> (Accessed: 18 May 2019).
- (Bond, D. 2019) *MI5 under fire for 'unlawful' handling of personal data*. Available at: <https://www.ft.com/content/986ebc26-8c49-11e9-a1c1-51bf8f989972> (Accessed: 3 November 2019)
- Borger, J. (2013) *NSA files: what's a little spying between old friends?* Available at: <https://www.theguardian.com/world/2013/dec/02/nsa-files-spying-allies-enemies-five-eyes-g8> (Accessed: 10 July 2018).
- Bossewitch, J. and Sinnreich, A. (2013) 'The end of forgetting: Strategic agency beyond the panopticon', *New Media & Society*, 15(2), pp. 224-242.
- Bowcott, O. (2015) *UK-US surveillance regime was unlawful 'for seven years'*. Available at: <https://www.theguardian.com/uk-news/2015/feb/06/gchq-mass-internet-surveillance-unlawful-court-nsa> (Accessed: 3 November 2019)
- Bowen, M. (2015) This Day in History: President Lyndon B. Johnson Signed the Civil Rights Act of 1964. Available at: <https://obamawhitehouse.archives.gov/blog/2015/07/02/day-history-president-lyndon-b-johnson-signed-civil-rights-act-1964> (Accessed: 2 November 2019).
- Boyle, K. and Mower, J. (2018) 'Framing terror: A content analysis of media frames used in covering ISIS', *Newspaper Research Journal*, 39(2), pp.205-219.
- Bradshaw, S. and Howard, P.N. (2017) *Troops, trolls and troublemakers: A global inventory of organized social media manipulation*. Available at: <http://blogs.oii.ox.ac.uk/politicalbots/wp-content/uploads/sites/89/2017/07/Troops-Trolls-and-Troublemakers.pdf> (Accessed: 27 May 2019).

Brandenburg, H. (2007) “‘Security at the Source’ Embedding journalists as a superior strategy to military censorship’, *Journalism Studies*, 8(6), pp. 948-963.

Bressan, S. (2019) *Can the EU Prevent Deepfakes From Threatening Peace?* Available at: <https://carnegieeurope.eu/strategieurope/79877> (Accessed: 2 January 2019)

Brewer, M.B and Crano, W. (1994) *Social Psychology*. Minneapolis: West Publishing Company.

Briant, E.L. (2015) ‘Allies and Audiences Evolving Strategies in Defense and Intelligence Propaganda’, *The International Journal of Press/Politics*, 20(2), pp. 145 – 165.

Brown, J. A. C. (1963) *Techniques of Persuasion: From Propaganda to Brainwashing*. Harmondsworth: Penguin.

Brown, K. (1995) ‘Intelligence and the decision to collect it: Churchill's wartime American diplomatic signals intelligence’, *Intelligence and National Security*, 10(3), pp. 449-467.

Browning, C.S. and Joenniemi, P. (2017) ‘Ontological security, self-articulation and the securitization of identity’, *Cooperation and Conflict*, 52(1), pp. 31-47.

Brügger, N. and Finnemann, N.O. (2013) ‘The Web and Digital Humanities: Theoretical and Methodological Concerns’, *Journal of Broadcasting & Electronic Media*, 57(1), pp. 66-80.

Burchill, S. (2013) ‘Liberalism’, In Burchill, S., Linklater, A., Devetak, R., Donnelly, J., Nardin, T., Paterson, M., Reus-Smit, C., True, J. 5<sup>th</sup> Rev. edn. *Theories of International Relations*. London: Palgrave Macmillan, pp. 57 -87.

Bush, G. (2002) *Text of President Bush's 2002 State of the Union Address*. Available at: <https://www.washingtonpost.com/wp-srv/onpolitics/transcripts/sou012902.htm?> (Accessed: 25 November 2019)

Cadwalladr, C. (2019) *The Vote Leave scandal, one year on: 'the whole thing was traumatic'*. Available at: <https://www.theguardian.com/uk-news/2019/mar/17/vote-leave-scandal-one-year-on-shahmir-sanni-whistleblower-cambridge-analytica> (Accessed: 14 November 2019)

Cabinet Office (UK), (2010) *National intelligence machinery*. Available at: [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/61808/nim-november2010.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/61808/nim-november2010.pdf) (Accessed: 2 November 2018).

Cabinet Office (UK), (2011) *The UK Cyber Security Strategy. Protecting and promoting the UK in a digital world*. Available at: [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/60961/uk-cyber-security-strategy-final.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf) (Accessed: 23 December 2018).

Cardozo, N. (2017[a]) *D.C. Circuit Court Issues Dangerous Decision for Cybersecurity: Ethiopia is Free to Spy on Americans in Their Own Homes*. Available at: <https://www.eff.org/de/deeplinks/2017/03/dc-circuit-court-issues-dangerous-decision-cybersecurity-ethiopia-free-spy?page=179> (Accessed: December 10 2017).

Cardozo, N. (2017[b]) *Can Foreign Governments Launch Malware Attacks on Americans Without Consequences?* Available at: <https://www.eff.org/deeplinks/2017/02/can-foreign-governments-launch-malware-attacks-americans-without-consequences> (Accessed: 28 September 2018)

Casciani, D. (2014) *The undercover cop, his lover, and their son*. Available at: <https://www.bbc.co.uk/news/magazine-29743857> (Accessed: 11 December 2019).

Castellino, J. (2009) *The end of the Liberal State: and the first Terrorist*. London: Middlesex University Press

CBS News (2019) *Crowd chants "send her back" at Trump rally, echoing president's tweets.*

Available at: <https://www.youtube.com/watch?v=sALwssmgB64> (Accessed: 7 November 2019)

Calamur, K. (2015) *Japan Says Sorry for Its Crimes Against Wartime 'Comfort Women'.*

Available at: <https://www.theatlantic.com/international/archive/2015/12/japan-korea-comfort-women/422016/> (Accessed: 9 September 2018).

Caparini, M. (2013) 'Controlling and Overseeing Intelligence Services in Democratic States',

in Born, H. and Caparini, M. (ed.) *Democratic control of intelligence services: Containing rogue elephants.* Aldershot: Ashgate Publishing, pp. 3-25.

Caplan, P. (2000) 'Introduction: Risk revisited' in Caplan, P. (ed.) *Risk Revisited.* London:

Pluto Press, pp. 1-28.

Carr, E.H. (1939) *The Twenty Years' Crisis, 1919-1939.* Rev. edn. London: Palgrave

Macmillan.

Carnegie Endowment (2019) *What Are Deepfakes?* Available at:

[https://www.youtube.com/watch?v=etSfYERBK28&feature=emb\\_logo](https://www.youtube.com/watch?v=etSfYERBK28&feature=emb_logo) (Accessed: 2 January 2020)

Casciani, D. (2018) *Metropolitan Police admits role in blacklisting construction workers.*

Available at: <http://www.bbc.co.uk/news/uk-43507728> (Accessed: 20th April 2018). #

Casetext (2019) *U.S. v. Hollingsworth. United States Court of Appeals, Seventh Circuit 9 F.3d*

593. Available at: <https://casetext.com/case/us-v-hollingsworth-8> (Accessed: 2 January 2020)

Castells, M. (2009) *Communication Power.* Oxford: Oxford University Press.

Catlin, G.E.G. (1935) 'The Rôle of Propaganda in a Democracy', *The Annals of the American Academy of Political and Social Science*, 179(1), pp.219-226.

Catlin, G.E.G. (1936) 'Propaganda as a Function of Democratic Government', in Childs, H.L. (ed.) *Propaganda and Dictatorship: A Collection of Papers*. New Jersey: Princeton University Press, pp.125-145.

Cavallar, G. (2012) 'Cosmopolitanisms in Kant's philosophy', *Ethics & Global Politics*, 5(2), pp.95-118.

Central Intelligence Agency (1954) *Division Project Clearance Sheet*. Available at: [https://www.cia.gov/library/readingroom/docs/DTLINEN-KGU%20%20%20VOL.%201\\_0064.pdf](https://www.cia.gov/library/readingroom/docs/DTLINEN-KGU%20%20%20VOL.%201_0064.pdf) (Accessed: 11 May 2019).

Central Intelligence Agency (1975) *Statement by Mr. Allen W. Dulles to the senate foreign relations committee*. Available at: [https://www.cia.gov/library/readingroom/docs/DOC\\_000009190.pdf](https://www.cia.gov/library/readingroom/docs/DOC_000009190.pdf) (Accessed: 24 April 2018).

Central Intelligence Agency (2012) *The Berlin Tunnel*. Available at: <https://www.cia.gov/about-cia/cia-museum/experience-the-collection/text-version/stories/the-berlin-tunnel.html> (Accessed: 24 April 2018).

Central Intelligence Agency (2013[a]) *INTelligence: Signals Intelligence*. Available at: <https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/intelligence-signals-intelligence-1.html> (Accessed: 22 December 2018).

Central Intelligence Agency (2013[b]) *The Office of Strategic Services: Morale Operations Branch*. Available at: <https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/oss-morale-operations.html> (Accessed: 14 May 2018).

Central Intelligence Agency (2013[c]) *OSS's WWII Anti-Axis Propaganda*. Available at: <https://www.cia.gov/news-information/featured-story-archive/2012-featured-story-archive/wwii-anti-axis-propaganda.html> (Accessed: 14 May 2018).

Central Intelligence Agency (2015) *CORONA: Declassified*. Available at: <https://www.cia.gov/news-information/featured-story-archive/2015-featured-story-archive/corona-declassified.html> (Accessed: 24 April 2018).

Central Intelligence Agency (2016[a]) *Human Intelligence*. Available at: <https://www.cia.gov/offices-of-cia/ clandestine-service/intelligence.html> (Accessed: 7 January 2018).

Central Intelligence Agency (2016[b]) *Morale Operations Field Manual- Strategic Services – Strategic Services (Provisional)*. Available from: <https://www.cia.gov/library/readingroom/docs/CIA-RDP89-01258R000100010002-4.pdf> (Accessed: 14 April 2018).

Central Intelligence Agency (2016[c]) *A Strategic Concept for Cold War Operations under NSC 10/5*. Available at: <https://www.cia.gov/library/readingroom/docs/CIA-RDP80R01731R003300080011-0.pdf> (Accessed: 26 June 2018).

Central Intelligence Agency (2016[d]) *Sino-Soviet Bloc Propaganda Forgeries 1 January 1957 to 1 July 1959*. Available at: <https://www.cia.gov/library/readingroom/docs/CIA-RDP78-02646R000300130001-0.pdf> (Accessed: 2 November 2017).

Central Intelligence Agency (2016[e]) *Soviet Active Measures' Forgery, Disinformation, Political Operations*. Available at: <https://www.cia.gov/library/readingroom/docs/CIA-RDP84B00049R001303150031-0.pdf> (Accessed: 20 November 2016).

Central Intelligence Agency (2016[f]) *The Soviet Forgery War*. Available at: <https://www.cia.gov/library/readingroom/docs/CIA-RDP84B00049R000902220014-7.pdf> (Accessed: 20 October 2017).

Central Intelligence Agency (2016[g]) *Errata*. Available at:

<https://www.cia.gov/library/readingroom/docs/CIA-RDP78-00915R001200080009-1.pdf> (Accessed: 2 November 2017).

Central Intelligence Agency (2016[h]) *Alleged KKK Death Threats To Third World Olympic Athletes: A Soviet Active Measure*. Available at:

<https://www.cia.gov/library/readingroom/docs/CIA-RDP85T00287R001400750001-6.pdf> (Accessed: 9 July 2018).

Central Intelligence Agency (2016[i]) *SE-24: Significance of the Communist Psychological Warfare Campaign Alleging Use of Biological Warfare by the US in Korea (Draft For Board Consideration)*. Available at:

<https://www.cia.gov/library/readingroom/docs/CIA-RDP79S01011A000600050029-8.pdf> (Accessed: 10 July 2018).

Central Intelligence Agency (n.d.) *DTLINEN*. Available at:

[https://www.cia.gov/library/readingroom/docs/DTLINEN\\_0052.pdf](https://www.cia.gov/library/readingroom/docs/DTLINEN_0052.pdf) (Accessed: 19 November 2017).

Chafer, T. (2005) 'Chirac and 'la Francafrique': No longer a family affair', *Modern & Contemporary France*, 13(1), pp. 7-23.

Chafer, T. and Cumming, G. (2010) 'Beyond Fashoda: Anglo-French security cooperation in Africa since Saint-Malo', *International Affairs*, 86(5), pp.1129-1147.

Channel 4 News, (2019) *Akala interview on institutional racism and knife crime*. Available at:

[https://www.youtube.com/watch?v=6Huz1nx-j\\_Q](https://www.youtube.com/watch?v=6Huz1nx-j_Q) (Accessed: 4 November 2019)

Charbonneau, L. (2013) *U.S. drone strikes violate Pakistan's sovereignty: U.N.* Available at:

<https://www.reuters.com/article/us-un-drones/u-s-drone-strikes-violate-pakistans-sovereignty-u-n-idUSBRE92E0Y320130316> (Accessed: 3 November 2019).



- Charters, D.A. (1977) 'Intelligence and psychological warfare operations in Northern Ireland', *The RUSI Journal*, 122(3), pp. 22-27.
- Charters, D.A. (2017) 'British intelligence in the Palestine campaign, 1945–47', *In Modern Counter-Insurgency*, 6(1), pp. 115-140.
- Chatterjee, D. (2016) 'Gendering ISIS and mapping the role of women', *Contemporary Review of the Middle East*, 3(2), pp.201-218.
- Chernobrov, D. (2016) 'Ontological security and public (mis) recognition of international crises: Uncertainty, political imagining, and the self', *Political Psychology*, 37(5), pp. 581-596.
- Chomsky, M. (2002) *Media Control. The Spectacular Achievements of Propaganda*. 2<sup>nd</sup> edn. New York: Seven Stories Press.
- Chomsky's Philosophy (2015) *Noam Chomsky – Unpeople*. Available at: [https://www.youtube.com/watch?v=ewac8VkQx\\_k](https://www.youtube.com/watch?v=ewac8VkQx_k) (Accessed: 2 December 2017).
- Chrisafis, A. (2016) *Paris attacks inquiry finds multiple failings by French intelligence agencies*. Available at: <https://www.theguardian.com/world/2016/jul/05/paris-attacks-inquiry-multiple-failings-french-intelligence-agencies> (Accessed: 20 April 2017).
- Cimpanu, C. (2018) *How US authorities tracked down the North Korean hacker behind WannaCry*. Available at: <https://www.zdnet.com/article/how-us-authorities-tracked-down-the-north-korean-hacker-behind-wannacry/> (Accessed: 6 November 2019).
- Clegg, N. (2019) *Facebook, Elections and Political Speech*. Available at: <https://about.fb.com/news/2019/09/elections-and-political-speech/> Accessed: (14 November 2019)

Climate Network Africa (2018) *Transformations to sustainability*. Available at:

<http://www.eldis.org/document/A102576> (Accessed: 11 November 2018).

CNN, (2003) *Bush declares war*. Available at:

<http://edition.cnn.com/2003/US/03/19/sprj.irq.int.bush.transcript/> (Accessed: 21 May 2019).

CNN (2009) *Italy convicts 'U.S. agents' in CIA kidnap trial*. Available at:

<http://edition.cnn.com/2009/WORLD/europe/11/04/italy.rendition.verdict/index.html>  
(Accessed: 3 November 2019)

CNN (2013) *Intelligence director admits spying on leaders*. Available at:

<https://www.youtube.com/watch?v=GzPSHywzadk> (Accessed: 29 September 2018).

CNN (2016[a]) *Obama: American Exceptionalism*. Available at:

<https://www.youtube.com/watch?v=95JiNT74Xtw> (Accessed: 16 November 2019)

CNN (2017[a]) *Warren agrees DNC was rigged against Sanders*. Available at:

<https://www.youtube.com/watch?v=I8qBexfR3r4> (Accessed: 8 July 2018).

CNN (2017[b]) *Warner: Russia tried electoral hack in 21 states*. Available at:

<https://www.youtube.com/watch?v=SW3pRek8Sm0> (Accessed: 25 May 2018).

CNN (2017[c]) *NSA chief: France warned about Russia hacking*. Available at:

<https://www.youtube.com/watch?v=lxupm7-zbK0> (Accessed: 9 July 2018).

CNN (2018) *GOP Sen. John Kennedy compares Putin to a shark*. Available at:

<https://www.youtube.com/watch?v=CQ52D5s805s> (Accessed: 3 January 2020)

CNN, (2019[a]) *Hear Fiona Hill's full opening impeachment hearing remarks*. Available at:

<https://www.youtube.com/watch?v=lZ3QmUJ4Bks&t=37s> (Accessed: 10 December 2019)

CNN, (2019[b]) Analyst: *Putin used to pay for trolls. Now, he has Ted Cruz*. Available at: <https://www.youtube.com/watch?v=-3RmHMg-0Pw&t=119s> (Accessed: 10 December 2019)

CNN (2019[c]) *Boston Marathon Terror Attack Fast Facts*. Available at: <https://edition.cnn.com/2013/06/03/us/boston-marathon-terror-attack-fast-facts/index.html> (Accessed: 25 April 2019).

Creemers, R. (2017) 'Cyber China: Upgrading Propaganda, Public Opinion Work and Social Management for the Twenty-First Century', *Journal of Contemporary China*, 26(103), pp. 85-100.

Croft, S. and Vaughan-Williams, N. (2016) 'Fit for purpose? Fitting ontological security studies 'into' the discipline of International Relations: Towards a vernacular turn', *Cooperation and Conflict*, 52(1), pp. 1-19.

Cohen, E.A. (2016) *The Chinese Intervention in Korea, 1950*. Available at: <https://www.cia.gov/library/readingroom/docs/1988-11-01.pdf> (Accessed: 27 February 2018).

Cold Spring Harbor Laboratory (n.d.) "*Comparison of white and negro fetuses*". Available at: <http://www.eugenicsarchive.org/html/eugenics/index2.html?tag=562> (Accessed: 12 November 2019)

Cold Spring Harbor Laboratory (2019) *Flashing light exhibit at Fitter Families Contests*. Available at: <https://dnalc.cshl.edu/view/10005-Flashing-light-exhibit-at-Fitter-Families-Contests.html> (Accessed: 12 November 2019)

Collinson, S. (2018) *Trump shocks with racist new ad days before midterms*. Available at: <https://edition.cnn.com/2018/10/31/politics/donald-trump-immigration-paul-ryan-midterms/index.html> (Accessed: 20 December 2018).

Combes, M.D. (2017) 'Encountering the stranger: Ontological security and the Boston Marathon bombing', *Cooperation and Conflict*, 52(1), pp. 126-143.

Commission Nationale de Contrôle de la Campagne électorale en vue de l'Élection Présidentielle, (2017) *RECOMMANDATION AUX MÉDIAS SUITE À L'ATTAQUE INFORMATIQUE DONT A ÉTÉ VICTIME L'ÉQUIPE DE CAMPAGNE DE M. MACRON*. Available at: <http://www.cncep.fr/communiqués/cp14.html#header> (Accessed: 4 November 2018).

Congress (US), (2015) *H.R.2048 - USA FREEDOM Act of 2015*. Available at: <https://www.congress.gov/bill/114th-congress/house-bill/2048/text> (Accessed: 8 December 2019)

Cook, I. (2008) *The Holocaust and disabled people: FAQ - frequently-asked questions*. Available at: [http://www.bbc.co.uk/ouch/fact/the\\_holocaust\\_and\\_disabled\\_people\\_faq\\_frequently\\_asked\\_questions.shtml](http://www.bbc.co.uk/ouch/fact/the_holocaust_and_disabled_people_faq_frequently_asked_questions.shtml) (Accessed: 5 December 2019).

Cornell Law School (n.d.[a]) *Sorrells v. United States*. Available at: <https://www.law.cornell.edu/supremecourt/text/287/435> (Accessed: 2 January 2020)

Cornell Law School (n.d.[b]) *Prisoners' rights*. Available at: [https://www.law.cornell.edu/wex/prisoners%27\\_rights](https://www.law.cornell.edu/wex/prisoners%27_rights) (Accessed: 2 January 2020)

Cory, C.E. (1919) 'A divided self', *The Journal of Abnormal Psychology*, 14(4), p.281 – 291

Court of Justice of the European Union (2014) *The Court of Justice declares the Data Retention Directive to be invalid*. Available at: <https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf> (Accessed: 9 May 2019).

Court of Justice of the European Union, (2019) *Judgment in Case C-507/17: Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés*

(CNIL). Available at: <https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-09/cp190112en.pdf> (Accessed: 7 December 2019)

C-Span (2018) *Speaker Ryan on Trump-Putin Meeting (C-SPAN)*. Available at <https://www.youtube.com/watch?v=qU140lx28l0> (Accessed: 3 January 2020)

Craig, A.J.S. and Valeriano, B. (2018) 'Realism and Cyber Conflict: Security in the Digital Age', in Orsi, D., Avgustin, J.R. and Nurnus, M. (eds.) *Realism in Practice*. Bristol: E-International Relations Publishing, pp. 85-101.

Crisp, R.J. and Turner, R.N (2010) *Essential Social Psychology*. Los Angeles : SAGE

Crown Prosecution Service, (2018) *Abuse of Powers*. Available at: <https://www.cps.gov.uk/legal-guidance/abuse-process> (Accessed: 18 December 2019)

Cullather, N. (1997) *Operation PBSUCCESS: The United States and Guatemala 1952-1954*. Available at: [https://www.cia.gov/library/readingroom/docs/DOC\\_0000134974.pdf](https://www.cia.gov/library/readingroom/docs/DOC_0000134974.pdf) (Accessed: 16 May 2018).

Cunliffe, W.H. (2016) *Select Documents on Japanese War Crimes and Japanese Biological Warfare, 1934-2006*. Available at: <https://www.archives.gov/files/iwg/japanese-war-crimes/select-documents.pdf> (Accessed: 5 November 5, 2018).

Cunningham, S.B. (2001) 'Responding to Propaganda: An Ethical Enterprise', *Journal of Mass Media Ethics*, 16(2-3), pp.138-147.

Dack, S. (2019) *Deep Fakes, Fake News, and What Comes Next*. Available at: <https://jsis.washington.edu/news/deep-fakes-fake-news-and-what-comes-next/> (Accessed: 24 May 2019).

Darwin, C. (1859) *On the Origin of Species by Means of Natural Selection, Or, The Preservation*. London: John Murray.

*Data Retention and Investigatory Powers Act 2014*, c. 27. Available at:

[http://www.legislation.gov.uk/ukpga/2014/27/pdfs/ukpga\\_20140027\\_en.pdf](http://www.legislation.gov.uk/ukpga/2014/27/pdfs/ukpga_20140027_en.pdf) (Accessed: 3 February 2019).

Davis, M. (2001) *Late Victorian Holocausts. El Nino Famines and the Making of the Third World*. London: Verso.

Davison, W.P. (1971) 'Some trends in international propaganda', *The ANNALS of the American Academy of Political and Social Science*, 398(1), pp. 1-13.

Dawes, S. (2015) 'Charlie Hebdo, Free Speech and Counter-Speech', *Sociological Research Online*, 20(3), pp.1-8.

Del Pero, M. (2001) 'The United States and "psychological warfare" in Italy, 1948-1955', *The Journal of American History*, 87(4), pp. 1304-1334.

Democracy Now (2016) *Report: Pentagon Paid PR Firm for Phony al-Qaeda Videos in Iraq*. Available at:

[https://www.democracynow.org/2016/10/3/headlines/report\\_pentagon\\_paid\\_pr\\_firm\\_for\\_phony\\_al\\_qaeda\\_videos\\_in\\_iraq](https://www.democracynow.org/2016/10/3/headlines/report_pentagon_paid_pr_firm_for_phony_al_qaeda_videos_in_iraq) (Accessed: 20 November 2017).

Department of Defense (US) (2015) *Beyond the Build Delivering Outcomes through Cyberspace The Commander's Vision and Guidance for US Cyber Command*. Available at: [https://dod.defense.gov/Portals/1/features/2015/0415\\_cyber-strategy/docs/US-Cyber-Command-Commanders-Vision.pdf](https://dod.defense.gov/Portals/1/features/2015/0415_cyber-strategy/docs/US-Cyber-Command-Commanders-Vision.pdf) (Accessed: 2 November 2017).

Department of Defense (US) (2018) *Summary Department of Defense Cyber Strategy*.

Available at: [https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER\\_STRATEGY\\_SUMMARY\\_FINAL.PDF](https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF) (Accessed: 14 December 2018).

- Department of Public Safety and Emergency (Canada) (2018) *Security and Prosperity in the Digital Age: Consulting on Canada's Approach to Cyber Security*. Available at: <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/2016-scrty-prsprty/index-en.aspx#a02> (Accessed: December 2018).
- DeYoung, K. and Nakashima. E. (2017) *UAE orchestrated hacking of Qatari government sites, sparking regional upheaval, according to U.S. intelligence officials*. Available at: [https://www.washingtonpost.com/world/national-security/uae-hacked-qatari-government-sites-sparking-regional-upheaval-according-to-us-intelligence-officials/2017/07/16/00c46e54-698f-11e7-8eb5-cbccc2e7bfbf\\_story.html?noredirect=on&utm\\_term=.2aeb02be906a](https://www.washingtonpost.com/world/national-security/uae-hacked-qatari-government-sites-sparking-regional-upheaval-according-to-us-intelligence-officials/2017/07/16/00c46e54-698f-11e7-8eb5-cbccc2e7bfbf_story.html?noredirect=on&utm_term=.2aeb02be906a) (Accessed: 3 June 2018).
- Diener, E. (1979) 'Deindividuation, self-awareness, and disinhibition', *Journal of Personality and Social Psychology*, 37(7), pp. 1160.
- Dietrich, D.J. (1992) 'Catholic eugenics in Germany, 1920-1945: Hermann Muckermann, SJ and Joseph Mayer', *Journal of Church & State*, 34(3) p.575.
- Dinges, J. (2005) *The Condor Years. How Pinochet And His Allies Brought Terrorism To Three Continents*. New York: The New Press.
- Dixon, M. (2013) *Textbook on International Law*. Oxford: Oxford University Press.
- Dockstader, J. (2018) 'Cynic cosmopolitanism', *European Journal of Political Theory*, 0(0), p.1-18.
- DocsTeach (n.d.) *Telegram with a Translation of the Zimmermann Telegram*. Available at: <https://www.docsteach.org/documents/document/translation-zimmermann-telegram> (Accessed: 1 March 2019).

Dodge, R. (1920) 'The Psychology of Propaganda', *Religious Education*, 15(5), pp. 241-252.

Donahue, E.M., Robins, R.W., Roberts, B.W. and John, O.P. (1993) 'The divided self: Concurrent and longitudinal effects of psychological adjustment and social roles on self-concept differentiation', *Journal of personality and social psychology*, 64(5), p.834.

Drezner, D.W. (2017) *White House aides can't stop talking about President Trump like he's a toddler [UPDATED]*. Available at: [https://www.washingtonpost.com/news/posteverything/wp/2017/08/21/the-trump-as-toddler-thread-explained-and-curated/?utm\\_term=.ac974bd1626a](https://www.washingtonpost.com/news/posteverything/wp/2017/08/21/the-trump-as-toddler-thread-explained-and-curated/?utm_term=.ac974bd1626a) (Accessed: 20 February 2019).

DW News (2019) *Hong Kong pro-democracy and pro-Beijing protesters clash at mall: DW News*. Available at: <https://www.youtube.com/watch?v=gwxiezDR1dg> (Accessed: 2 January 2020)

Echikson, W. and Knodt, O. (2018) *Germany's NetzDG: A key test for combatting online hate*. Available at: [https://www.ceps.eu/system/files/RR%20No2018-09\\_Germany%27s%20NetzDG.pdf](https://www.ceps.eu/system/files/RR%20No2018-09_Germany%27s%20NetzDG.pdf) (Accessed: 8 December 2019)

Easter, D. (2005) 'Keep the Indonesian pot boiling': Western covert intervention in Indonesia', October 1965–March 1966', *Cold War History*, 5(1), pp. 55-73.

Easterly, W. (2006) *The White Mans Burden: Why The West's Efforts To Aid The Rest Have Done So Much Ill And So Little Good*. Oxford: Oxford University Press.

Eden, A. (1956) 'Commander Crabb (Presumed Death)', *Hansard: House of Commons Debate*, 9 May, 552 cc1220-3. Available at: [https://api.parliament.uk/historic-hansard/commons/1956/may/09/commander-crabb-presumed-death-1#column\\_1220](https://api.parliament.uk/historic-hansard/commons/1956/may/09/commander-crabb-presumed-death-1#column_1220) (Accessed: 1 March 2019).



Edwards, A. (2015) 'ISIS and the challenge of Islamist extremism', *Political Insight*, 6(1), pp.12-15.

Edwards, D. and Potter, J. (1992) *Discursive psychology*. London: Sage publications Ltd.

Electronic Frontier Foundation (n.d.) *The Playpen Cases: Frequently Asked Questions*.

Available at: <https://www.eff.org/pages/playpen-cases-frequently-asked-questions#whathappened> (Accessed: 10 December 2019)

Electronic Frontier Foundation (2013[a]) *Computer Network Operations (U) SIGINT Enabling*:

Available at: <https://www.eff.org/tr/document/2013-09-05-guard-sigint-enabling> (Accessed: 8 December 2017).

Electronic Frontier Foundation (2013[b]) *iPhone Location Services*. Available at:

<https://www.eff.org/files/2013/11/15/20130909-spiegel-smartphones.pdf> (Accessed: 18 April 2018).

Electronic Frontier Foundation (2014[a]) *Full Spectrum Cyber Effects*. Available at:

[https://www.eff.org/files/2014/04/09/20140404-intercept-gchq\\_full\\_spectrum\\_cyber\\_effects.pdf](https://www.eff.org/files/2014/04/09/20140404-intercept-gchq_full_spectrum_cyber_effects.pdf) (Accessed: 5 June 2019).

Electronic Frontier Foundation (2014[b]) *King*. Available at:

<https://www.eff.org/files/2014/11/12/mlkletters.jpg> (Accessed: 3 January 2017).

Electronic Frontier Foundation (2014[c]) *20140714-Intercept-GCHQ's Joint Threat Research*

*Intelligence Group*. Available at: <https://www.eff.org/document/20140714-intercept-gchqs-joint-threat-research-intelligence-group> (Accessed: 12 July 2018).

Electronic Frontier Foundation (2014[d]) *GCHQ Presentation on the BULLRUN Programs*

*Decryption Capabilities*. Available at: <https://www.eff.org/ar/document/20141228-spiegel-gchq-presentation-bullrun-programs-decryption-capabilities> (Accessed: 2 November 2017).

Ellul, J. (1973) *Propaganda: The Formation of Men's Attitudes*. Translated by Kellen, K. and Lerner, J. New York: Vintage Books.

Ellul, J. (1965) *The Technological Society*. Translated by Wilkinson, J. Rev. edn. London: Johnathan Cape.

Elsayed-Ali, S. (2015) *10 spy programmes with silly codenames used by GCHQ and NSA*. Available at: <https://www.amnesty.org/en/latest/campaigns/2015/03/10-spy-programmes-with-silly-codenames-used-by-gchq-and-nsa/> (Accessed: 17 December 2018).

Elsa, J.K., Schwartz, M. and Nakamura, K.H. (2008) *Private Security Contractors in Iraq: Background, Legal Status, and Other Issues*. Available at: <https://fas.org/sgp/crs/natsec/RL32419.pdf> (Accessed: 2 January 2020)

Embassy of France in London (2018[a]) *Fight against terrorism – G5 Sahel – Communiqué issued by the Ministry for the Armed Forces*. Available at: <https://uk.ambafrance.org/France-Mali-and-Mauritania-conduct-anti-terror-operation> (Accessed: 14 December 2018).

Embassy of France in London (2018[b]) *Fight against terrorism – Syria/Iraq/G5 Sahel – Interview given by Mme Florence Parly, Minister for the Armed Forces, to the daily newspaper Libération website*. Available at: <https://uk.ambafrance.org/Armed-Forces-Minister-explains-French-policy> (Accessed: 14 December 2018).

Eric Swalwell (2017) *Swalwell's Statement on GOP Efforts to Distract from Russia Investigation*. Available at: <https://swalwell.house.gov/media-center/press-releases/swalwells-statement-gop-efforts-distract-russia-investigation> (Accessed: 24 May 2018).

Esslemont, T. (2016) *United Nations must act to end sex abuse 'cover-ups': whistleblower*.

Available at: <https://www.reuters.com/article/us-un-whistleblower-sexabuse-idUSKCN0V021L> (Accessed: 9 May 2019).

Esterberg, K.G. (2002) *Qualitative Methods in Social Research*. Boston: McGraw-Hill.

Estrada, A. (2015) *The Politics of Female Biology and Reproduction*. Available at:

<https://www.news.ucsb.edu/2015/015287/politics-female-biology-and-reproduction>  
(Accessed: 10 November 2019)

EU Factcheck (2019) *Fact-Checks*. Available at: <https://eufactcheck.eu/fact-checks/>

(Accessed: 2 January 2020)

EUNAVFOR Somalia (2018) *Mission*. <https://eunavfor.eu/mission/> (Accessed: 14 December 2018).

EUR-LEX (2006) *Directive 2006/24/EC of the European Parliament and of the Council of 15*

*March*. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32006L0024&from=EN> Accessed: 1 July 2015).

EUR-Lex, (2012) *Charter of Fundamental Rights of The European Union*. Available at:

<https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012P/TXT&from=EN> (Accessed: 30 November 2019)

European Parliament (2010) *Kenya: failure to arrest President Omar al-Bashir of Sudan*.

Available at:

<http://www.europarl.europa.eu/document/activities/cont/201009/20100917ATT82761/20100917ATT82761EN.pdf> (Accessed: 1 January 2020)

European Parliament (2017) *The Impact of Schemes revealed by the Panama Papers on the Economy and Finances of a Sample of Member States*. Available at:

[http://www.europarl.europa.eu/RegData/etudes/STUD/2017/572717/IPOL\\_STU\(2017\)572717\\_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2017/572717/IPOL_STU(2017)572717_EN.pdf) (Accessed: 10 July 2018).

European Parliament (2018) *Third Facebook-Cambridge Analytica hearing: data breach prevention and cures*. Available at: <https://www.europarl.europa.eu/news/en/press-room/20180702IPR07037/third-facebook-cambridge-analytica-hearing-data-breach-prevention-and-cures> (Accessed: 2 January 2020)

European Union External Action (2018) *EU Training Mission in Mali (EUTM Mali)*. Available at: [http://eeas.europa.eu/archives/docs/csdp/missions-and-operations/eutm-mali/pdf/factsheet\\_eutm\\_mali\\_en.pdf](http://eeas.europa.eu/archives/docs/csdp/missions-and-operations/eutm-mali/pdf/factsheet_eutm_mali_en.pdf) (Accessed: 14 December 2018).

Europol (2017) *Major Online Child Sexual Abuse Operation Leads to 368 Arrests in Europe*. Available at: <https://www.europol.europa.eu/newsroom/news/major-online-child-sexual-abuse-operation-leads-to-368-arrests-in-europe> (Accessed: 10 December 2019).

Evans, G. and Newnham, J. (1998) *The Penguin Dictionary of International Relations*. Harmondsworth: Penguin.

Facebook (2017) *An Update On Information Operations On Facebook*. Available at: <https://newsroom.fb.com/news/2017/09/information-operations-update/> (Accessed: at 20 February 2017).

Facebook Newsroom, (2019) *Removing Coordinated Inauthentic Behavior From China*. Available at: <https://newsroom.fb.com/news/2019/08/removing-cib-china/> (Accessed: 25 October 2019)

Fahmy, S. and Johnson, T.J. (2007) 'Embedded versus unilateral perspectives on Iraq War,' *Newspaper Research Journal*, 28(3), pp. 98-114.

Fairclough, N. (2010) *Critical Discourse Analysis: The Critical Study of Language*. 2nd edn. Harlow: Longman Group

Falklands Island Government (2012) *Our History*. Available at:

<https://www.falklands.gov.fk/our-people/our-history/> (Accessed: 26 April 2020)

Farber, S.A. (2008) 'US Scientists' Role in the Eugenics Movement (1907–1939): A Contemporary Biologist's Perspective', *Zebrafish*, 5(4), pp.243-245.

Federation of American Scientists (2005) *Psychological Operations*. Available at:

<https://fas.org/irp/doddir/army/fm3-05-30.pdf> (Accessed: 18 August 2018).

Federation of American Scientists (n.d.[a]) *Counter Intelligence in World War II*. Available at:

[https://fas.org/irp/ops/ci/docs/ci2/2ch4\\_a.htm](https://fas.org/irp/ops/ci/docs/ci2/2ch4_a.htm) (Accessed: 23rd April 2018).

Federation of American Scientists (n.d.[b]) *POPPY Program Fact Sheet*. Available at:

<https://fas.org/irp/nro/poppy.pdf> (Accessed 6 November 2018).

Federal Bureau of Investigation (n.d.[a]) *Intelligence Branch*. Available at:

<https://www.fbi.gov/about/leadership-and-structure/intelligence-branch> (Accessed: 22 December 2018) (Intelligence definition).

Federal Bureau of Investigation (n.d.[b]) *Ana Montes: Cuban Spy*. Available at:

<https://www.fbi.gov/history/famous-cases/ana-montes-cuba-spy> (Accessed: 23 April 2018).

Federal Bureau of Investigation (n.d.[c]) *Terrorism*. Available at:

<https://www.fbi.gov/investigate/terrorism#Terrorism-Definitions> (Accessed: 27 May 2019).

Federal Bureau of Investigation (1958[a]) *SOLO Part 02 of 125*. Available at:

<https://vault.fbi.gov/solo/solo-part-02-of/view> (Accessed: 11 July 2018).

Federal Bureau of Investigation (1958[b]) *SOLO Part 01 of 125*. Available at:  
<https://vault.fbi.gov/solo/solo-part-01-of/view> (Accessed: 11 July 2018).

Federal Bureau of Investigation (1967) *COINTELPRO Black Extremist Part 01 of 23*.  
Available at: <https://vault.fbi.gov/cointel-pro/cointel-pro-black-extremists/cointelpro-black-extremists-part-01-of/view> (Accessed: 20 November 2016).

Federal Bureau of Investigation (1968[a]) *SOLO Part 125 of 125*. Available at:  
<https://vault.fbi.gov/solo/solo-part-125-of-125/view> (Accessed: 11 July 2018).

Federal Bureau of Investigation (1968[b]) *COINTELPRO Black Extremist Part 13 of 23*.  
Available at: <https://vault.fbi.gov/cointel-pro/cointel-pro-black-extremists/cointelpro-black-extremists-part-10-of/view> (Accessed 5 November 2018).

Federal Bureau of Investigation (1969) *COINTELPRO Black Extremist Part 20 of 23*.  
Available at: <https://vault.fbi.gov/cointel-pro/cointel-pro-black-extremists/cointelpro-black-extremists-part-14/view> (Accessed: 5 November 2018).

Federal Bureau of Investigation (2014) *Update on Sony Investigation*. Available at:  
<https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation>  
(Accessed: 4 November 2018).

Federal Bureau of Investigation (2015) *Counterterrorism Policy Directive and Policy Guide*.  
Available at: <https://www.documentcloud.org/documents/3423189-CT-Excerpt.html#document/p16/a336266> (Accessed: 2 November 2018).

Federal Bureau of Investigation, (2017) *'Playpen' Creator Sentenced to 30 Years*. Available  
at: <https://www.fbi.gov/news/stories/playpen-creator-sentenced-to-30-years> (Accessed:  
10 December 2019)

- Feldstein, S. (2019) *The Global Expansion of AI Surveillance*. Available at: <https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847> (Accessed: 25 October 2019).
- Festinger, I., Pepitone, A. and Newcomb, T. (1952) 'Some consequences of deindividuation in a group', *Journal of Abnormal and Social Psychology*, 47(2), pp. 382-389.
- Fidler, D.P. (2015) *The Snowden Reader*. Bloomington: Indiana University Press.
- Fielding-Smith, A., Black, C. and Ungood-Thomas, J. (2016) *Soap operas and fakery: selling peace in Iraq*. Available at: <https://www.thetimes.co.uk/article/soap-operas-and-fakery-selling-peace-in-iraq-h5m5sscr9> (Accessed: 20 November 2017).
- Finch, L. (2000) 'Psychological propaganda: The war of ideas on ideas during the first half of the twentieth century', *Armed Forces & Society*, 26(3), pp. 367-386.
- FireEye, (2017) *Senate Intelligence Committee: Russia and 2016 Election*. Available at: <https://www.fireeye.com/content/dam/fireeye-www/solutions/pdfs/st-senate-intel-committee-russia-election.pdf> (Accessed: 8 December 2019)
- FireEye (2018) *Suspected Iranian Influence Operations. Leveraging Inauthentic News Sites and Social Media Aimed at U.S., U.K., Other Audiences*. Available at: <https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-FireEye-Iranian-IO.pdf> (Accessed: 21 November 2018).
- Fishman, A. and Greenwald, G. (2015) *Britain Used Spy Team to Shape Latin American Public Opinion on Falklands*. Available at: <https://theintercept.com/2015/04/02/gchq-argentina-falklands/> (Accessed: 25 June 2018).
- Flick, U. (2014) *An Introduction To Qualitative Research*. 5<sup>th</sup> edn. London: SAGE.
- Flick, U. (2015) *Introducing research methodology*. London: SAGE.

Fleiner, T. (1999) *What are human rights?* Sydney: The Federation Press.

Fordham Law School Center on National Security (2017) *The American Exception Terrorism Prosecutions in the United States: The ISIS Cases March 2014 – August 2017*.

Available at: <https://news.law.fordham.edu/wp-content/uploads/2017/09/TheAmericanException9-17.pdf> (Accessed: 28 December 2017).

Foreign and Commonwealth Office., Her majesty's Treasury., Hunt, J., and Hammond, P.

(2018) *Iran Nuclear Deal: joint statement by UK, France and Germany*. Available at: <https://www.gov.uk/government/news/joint-statement-by-the-uk-france-and-germany-on-the-iran-nuclear-deal> (Accessed: 12 February 2019).

Forelle, M., Howard, P., Monroy-Hernández, A. and Savage, S. (2015) *Political bots and the manipulation of public opinion in Venezuela*. Available at:

<https://arxiv.org/ftp/arxiv/papers/1507/1507.07109.pdf> (Accessed: 2 November 2018).

Foucault, M. (1991) *Discipline and Punish. The Birth of the Prison*. London: Penguin.

Fox, J. (n.d.) *World War One propaganda*. Available at: <https://www.bl.uk/world-war-one/videos/world-war-one-propaganda> (Accessed: 1 January 2019).

France 24 (2009) *AU votes against cooperating with ICC arrest warrant for Bashir*. Available at: <https://www.france24.com/en/20090703-au-votes-against-cooperating-with-icc-arrest-warrant-bashir-> (Accessed: 1 January 2020)

France 24 (2017[a]) *One policeman, one attacker killed in Champs-Élysées shooting in Paris*. Available at: <https://www.france24.com/en/20170420-reports-shots-fired-champs-elysee-paris-police-guns-france> (Accessed: 25 April 2019).



France 24 (2017[b]) *How we debunked rumours that Macron has an offshore account.*

Available at: <http://observers.france24.com/en/20170505-france-elections-macron-lepen-offshore-bahamas-debunked> (Accessed: 7 July 2018).

France 24 (2018) *Turkey slams 'unacceptable' French comments over Khashoggi probe.*

Available at: <https://www.france24.com/en/20181112-turkey-slams-unacceptable-french-comments-over-khashoggi-probe> (Accessed: 28 April 2019).

France Diplomatie (2018) *G5 Sahel Joint Force and the Sahel Alliance.* Available at:

<https://www.diplomatie.gouv.fr/en/french-foreign-policy/defence-security/crisis-and-conflicts/g5-sahel-joint-force-and-the-sahel-alliance/> (Accessed: 14 December 2018).

France Diplomatie (2019) *Cybersecurity: Paris Call of 12 November 2018 for Trust and*

*Security in Cyberspace.* Available at: <https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in> (Accessed: 15 November 2019)

Frank, T. (2018) *JP Morgan reportedly had to oust a security chief backed by Palantir after executives found out he was spying on them.* Available at:

<https://www.cnbc.com/2018/04/19/jp-morgan-reportedly-had-to-oust-a-security-chief-backed-by-palantir.html> (Accessed: November 14 2019).

Fraser, N., O'Leary, J., Cannon, V. and Plan, F. (2018) *APT38: Details on New North Korean Regime-Backed Threat Group.* Available at: <https://www.fireeye.com/blog/threat-research/2018/10/apt38-details-on-new-north-korean-regime-backed-threat-group.html>

(Accessed: 4 November 2018).

Freeman, F. (2017) *Human Rights.* 3<sup>rd</sup> edn. Cambridge : Polity Press.

Fulcher, J. and Scott, J. (2011) *Sociology.* Oxford: Oxford University Press.

- Fung, B. (2016) *The British are frantically Googling what the E.U. is, hours after voting to leave it*. Available at: <https://www.washingtonpost.com/news/the-switch/wp/2016/06/24/the-british-are-frantically-googling-what-the-eu-is-hours-after-voting-to-leave-it/> (Accessed: 7 November 2019)
- G7 (2017) *G7 Declaration on Responsible States Behavior in Cyberspace*. Available at: [http://www.esteri.it/mae/resource/doc/2017/04/declaration\\_on\\_cyberspace.pdf](http://www.esteri.it/mae/resource/doc/2017/04/declaration_on_cyberspace.pdf) (Accessed: 28 December 2017).
- Gallacher, J.D., Kaminska, M., Kollanyi, B. and Howard, P.N. (2017) *Junk News and Bots during the 2017 UK General Election: What Are UK Voters Sharing Over Twitter?* Available at: <http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Junk-News-and-Bots-during-the-2017-UK-General-Election.pdf> (Accessed: 3 January 2019).
- Gallagher, R. (2015) *Profiled: From Radio to Porn, British Spies Track Web Users' Online Identities*. Available at: <https://theintercept.com/2015/09/25/gchq-radio-porn-spies-track-web-users-online-identities/> (Accessed: 17 May 2020)
- Gallagher, R. and Hager, N. (2015) *New Zealand Spies on Neighbours In Secret "Five Eyes" Global Surveillance*. Available at: <https://theintercept.com/2015/03/04/new-zealand-gcsb-surveillance-waihopai-xkeyscore/> (Accessed: 2 November 2018).
- Gall, C. (2018) *In Khashoggi Disappearance, Turkey's Slow Drip of Leaks Puts Pressure on Saudis*. Available at: <https://www.nytimes.com/2018/10/19/world/europe/turkey-khashoggi-saudi-arabia.html> (Accessed: 1 March 2019).
- Galton, F. (1907) *Inquires Into Human Faculty and Its Development*. Available at: <http://galton.org/books/human-faculty/FirstEdition/humanfacultydeve00galt.pdf> (Accessed: 5 November 2019).

- Garraway, A. and Smith. B. (2017) *Russian interference in UK politics and society*. Available at: <http://researchbriefings.parliament.uk/ResearchBriefing/Summary/CDP-2017-0255> (Accessed: 12 July 2018).
- Garrido, M.V. (2015) 'Contesting a biopolitics of information and communications: The importance of truth and sousveillance after Snowden', *Surveillance & Society*, 13(2), pp.153-167.
- Gendron, A. (2005) 'Just war, just intelligence: An ethical framework for foreign espionage', *International Journal of Intelligence and CounterIntelligence*, 18(3), pp. 398-434.
- Geoffrey, R. (2012) *Crimes Against Humanity : The Struggle for Global Justice*. 4<sup>th</sup> edn. London : Penguin
- Georgetown University (n.d.) Buck v Bell, one of the Supreme Court's worst mistakes. Available at: <https://bioethics.georgetown.edu/2016/02/buck-v-bell-one-of-the-supreme-courts-worst-mistakes/> (Accessed: 12 November 2019)
- George W Bush white House Archives (2004) Dr. Rice Addresses War on Terror. Available at: <https://georgewbush-whitehouse.archives.gov/news/releases/2004/08/20040819-5.html> (Accessed: 25 May 2019).
- Giddens, A. (1990) *The consequences of modernity*. Stanford, CA: Stanford University Press.
- Giddens, A. (1991) *Modernity and self-identity: Self and society in the late modern age*. Cambridge: Polity.
- Giles, L.F. (2005) *The Gulf of Tonkin Mystery: The SIGINT Hounds Were Howling*. Available at: [https://www.nsa.gov/Portals/70/documents/news-features/declassified-documents/gulf-of-tonkin/articles/release-2/rel2\\_thoughts\\_intelligence.pdf](https://www.nsa.gov/Portals/70/documents/news-features/declassified-documents/gulf-of-tonkin/articles/release-2/rel2_thoughts_intelligence.pdf) (Accessed: 1 March 2019).

- Giles, K. (2016) *Russia's 'New' Tools for Confronting the West Continuity and Innovation in Moscow's Exercise of Power*. Available at: <https://www.chathamhouse.org/sites/default/files/publications/2016-03-russia-new-tools-giles.pdf> (Accessed: 27 November 2018).
- Giles, K. (2017) *Countering Russian Information Operations in the Age of Social Media*. Available at: <https://www.cfr.org/report/countering-russian-information-operations-age-social-media> (Accessed: 25 October 2018)
- Goel, V., Singh, K. and Yasir, S. (2019) *India Shut Down Kashmir's Internet Access. Now, 'We Cannot Do Anything.'* Available at: <https://www.nytimes.com/2019/08/14/technology/india-kashmir-internet.html> (Accessed: 15 November 2019).
- Gonçalves, J.B. (2014) 'The spies who came from the tropics: intelligence services and democracy in Brazil', *Intelligence and National Security*, 29(4), pp. 581-599.
- Good Morning Britain (2019) *Tory Nicky Morgan Challenged Over '50,000 New Nurses' Pledge: Good Morning Britain*. Available at: <https://www.youtube.com/watch?v=CpcY6HsGmAM> (Accessed: 6 November 2019)
- Google (n.d.) *United States national security requests*. Available at: <https://transparencyreport.google.com/user-data/us-national-security> (Accessed: 27 April 2018).
- Government Publishing Office (US), (2004) *Intelligence Reform and Terrorism Prevention Act 2004*. Available at: <https://www.govinfo.gov/content/pkg/PLAW-108publ458/pdf/PLAW-108publ458.pdf> (Accessed: 14 December 2019)
- Government Publishing Office (US) (2011) *Title 28 - JUDICIARY AND JUDICIAL PROCEDURE*. Available at: <https://www.gpo.gov/fdsys/pkg/USCODE-2011-title28/html/USCODE-2011-title28-partIV-chap97.htm> (Accessed: 28 September 2019)

- Grayzel, S. (2014) *Women at Home in a World at War*. Available at: <https://www.bl.uk/world-war-one/articles/women-at-home> (Accessed 26 October 2018).
- Greenberg, S. B. (2018) *Riling Up the Base May Backfire on Trump*. Available at: <https://www.nytimes.com/2018/06/18/opinion/trump-base-midterms-moderate-republicans.html> (Accessed: 20 December 2018).
- Green, P and Ward, T. (2012) 'State Crime: A Dialectical View' in Maguire, M., Morgan, R. and Reiner, R. (ed) *The Oxford handbook of criminology*. 5<sup>th</sup> edn. Oxford: Oxford University Press, pp. 717 – 740.
- Greenwald, G. (2014[a]) How Covert Agents Infiltrate the Internet to Manipulate, Decieve, and Destroy Reputations. Available at: <https://theintercept.com/2014/02/24/jtrig-manipulation/> (Accessed: 5 June 2019).
- Greenwald, G. (2014[b]) *No Place to Hide: Edward Snowden, the NSA and the Surveillance State*. London: Penguin Group.
- Greenwald, G. (2014[c]) *The "Cuban Twitter" Scam Is a Drop in the Internet Propaganda Bucket*. Available at: <https://theintercept.com/2014/04/04/cuban-twitter-scam-social-media-tool-disseminating-government-propaganda/> (Accessed: 10 July 2018).
- Greenwald, G. and Gallagher, R. (2014) How the NSA Plans to Infect 'Millions' of Computers With Malware. Available at: <https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/> (Accessed: 14 February 2018).
- Grewal, P. (2018) *Suspending Cambridge Analytica and SCL Group From Facebook*. Available at: <https://about.fb.com/news/2018/03/suspending-cambridge-analytica/> (Accessed: 14 November 2019)

- Grieco, J.M. (1988) 'Anarchy and the limits of cooperation: a realist critique of the newest liberal institutionalism', *International organization*, 42(3), pp. 485-507.
- Groll, E. (2016) *Turns Out You Can't Trust Russian Hackers Anymore*. Available at: <https://foreignpolicy.com/2016/08/22/turns-out-you-cant-trust-russian-hackers-anymore/> (Accessed: 5 July 2018).
- Gunkel, D. J. (2005) 'Editorial: introduction to hacking and hacktivism', *New Media & Society*, 7(5), pp. 595-597.
- Gunter, B. (2009) 'The Public and Media Coverage of the War on Iraq', *Globalizations*, 6(1), pp. 41-60.
- Gustafsson, K. (2014) 'Memory politics and ontological security in Sino-Japanese relations', *Asian Studies Review*, 38(1), pp. 71-86.
- Hack, K. (1999) 'British intelligence and counter-insurgency in the era of decolonisation: The example of Malaya', *Intelligence and National Security*, 14(2), pp.124-155.
- Hafner, J. (2019) *Alex Jones called Sandy Hook shooting a hoax. Now the victims' parents can depose him*. Available at: <https://eu.usatoday.com/story/news/2019/02/14/alex-jones-infowars-sandy-hook-lawsuit-case-deposition-deposed/2868829002/> (Accessed: 1 January 2020)
- Haggerty, K.D. and Ericson, R.V. (2000) 'The surveillance assemblage', *The British journal of sociology*, 51(4), pp. 605-622.
- Haggerty, K. D. (2006[a]) 'Visible War: Surveillance, Speed, and Information War' in Haggerty, K.D. and Ericson, R. V. (ed.) *The New Politics of Surveillance And Visibility*. Toronto: University of Toronto Press Incorporated, pp. 250 -268.

- Haggerty, K.D. (2006[b]) 'Tear down the walls on demolishing the panopticon' in Lyon, D. (ed.) *Theorizing Surveillance: The panopticon and beyond*. Devon: Willian Publishing, pp. 23-45.
- Han, R. (2015) 'Manufacturing Consent in Cyberspace: China's "Fifty-Cent Army"', *Journal of Current Chinese Affairs*, 44(2), pp. 105-135.
- Hanson, J.S. (1996) 'Entrapment in cyberspace: a renewed call for reasonable suspicion', *The University of Chicago Legal Forum*, p.535-552
- Hanyok, R. J. (2005) *Skunks Bogies, Silent Hounds, and the Flying Fish: The Gulf of Tonkin Mystery, 2-4 August 1964*. Available at: <https://nsarchive2.gwu.edu//NSAEABB/NSAEABB132/relea00012.pdf> (Accessed: 19 August 2018).
- Haslam, N., Rothschild, L. and Ernst, D. (2002) 'Are essentialist beliefs associated with prejudice?', *British Journal of Social Psychology*, 41(1), pp.87-100.
- Haste, C. (1977) *Keep the Home Fires Burning Propaganda In the First World War*. London: Allen Lane.
- Havercroft, J. and Prichard, A. (2017) 'Anarchy and International Relations theory: A reconsideration', *Journal of International Political Theory*, 13(3), pp. 252-265.
- Hawkins, R.L. and Maurer, K. (2011) 'You fix my community, you have fixed my life': the disruption and rebuilding of ontological security in New Orleans', *Disasters*, 35(1), pp.143-159.
- Hay, B. (2005) 'Sting operations, undercover agents, and entrapment', *Missouri Law Review.*, 70(2), p.387-432.

- Helmus, T.C., Bodine-Baron, E., Radin, A., Magnuson, M., Mendelsohn, J., Marcellino, W., Bega, A. and Winkelman, Z. (2018) Russian social media influence: Understanding Russian Propaganda in Eastern Europe. Santa Monica: Rand Corporation. Available at: [https://www.rand.org/content/dam/rand/pubs/research\\_reports/RR2200/RR2237/RAND\\_RR2237.pdf](https://www.rand.org/content/dam/rand/pubs/research_reports/RR2200/RR2237/RAND_RR2237.pdf) (Accessed: 20 December 2019)
- Henderson, E.H. (1943) 'Toward a definition of propaganda', *The Journal of Social Psychology*, 18(1), pp.71-87.
- Herman, M. (2004). 'Ethics and intelligence after September 2001', *Intelligence & National Security*, 19(2), pp. 342-358.
- Hernandez, V and BBC Mundo, (2012) *Argentine Mothers mark 35 years marching for justice*. Available at: <https://www.bbc.co.uk/news/world-latin-america-17847134> (3 November 2019)
- Hewitt, B. A. (2010) 'Ontological Insecurity', in Jackson, R. L. and Hogg, M. A. (ed.) *Encyclopaedia of Identity*. Los Angeles: SAGE Inc, pp. 511 – 512.
- Hewstone, M. and Martin, R. (2008) 'Social Influence' in Hewstone, M., Stroebe, W. and Jonas. K. 4<sup>th</sup> edn. *Introduction to Social Psychology a European Perspectives*. Malden: Blackwell, pp. 216- 243.
- Heywood, A. (2011) *Global Politics*. Basingstoke: Palgrave Macmillan
- Heywood, A. (2014) *Global Politics*. 2<sup>nd</sup> edn. Basingstoke: Palgrave Macmillan
- Hillebrand, C. (2012) 'The role of news media in intelligence oversight', *Intelligence and National Security*, 27(5), pp. 689-706.
- Hinton, P.R. (2000) *Stereotypes, cognition, and culture*. London: Routledge.



Hobbes, T. (1991) *Leviathan*. In Tuck, R. (ed.). Rev. edn. Cambridge: Cambridge University Press, pp. 86 – 115.

Hochwald, T. (2013) ‘How Do Social Media Affect Intra-State Conflicts other than War?’ *Connections*, 12(3), pp. 9-38.

Hogg, M. A. and Vaughan, G.M (2018) *Social Psychology*. 8<sup>th</sup> edn. Harlow: Pearson

Holpuch, A. (2019) US immigration police broke Facebook rules with fake profiles for college sting. Available at: <https://www.theguardian.com/technology/2019/apr/11/us-immigration-police-broke-facebook-rules-with-fake-profiles-for-college-sting> (Accessed, 18 May 2019).

Home Office (2015[a]) *Communications data*. Available at: <https://www.gov.uk/government/collections/communications-data> (Accessed: 13 February 2019).

Home Office (2015[b]) *Revised Prevent Duty Guidance: for England and Wales*. Available at: [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/445977/3799\\_Revised\\_Prevent\\_Duty\\_Guidance\\_England\\_Wales\\_V2-Interactive.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/445977/3799_Revised_Prevent_Duty_Guidance_England_Wales_V2-Interactive.pdf) (Accessed: January 10 2018).

Home Office (2018) *CONTEST: The United Kingdom’s Strategy for Countering Terrorism*. Available at: [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/716907/140618\\_CCS207\\_CCS0218929798-1\\_CONTEST\\_3.0\\_WEB.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/716907/140618_CCS207_CCS0218929798-1_CONTEST_3.0_WEB.pdf) (Accessed: 11 May 2019).

Hough, P. (2013) *Understanding Global Security*. 3<sup>rd</sup> edn. Oxon: Routledge.

House of Commons (2015[a]) *Investigatory Powers Bill: factsheet – bulk equipment interference*. Available

at:[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/473753/Factsheet-Bulk\\_Equipment\\_Interference.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/473753/Factsheet-Bulk_Equipment_Interference.pdf) URL (Accessed: 12 February 2019).

House of Commons (2015[b]) *Factsheet – Targeted Equipment Interference*. Available at: [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/473740/Factsheet-Targeted\\_Equipment\\_Interference.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/473740/Factsheet-Targeted_Equipment_Interference.pdf) (Accessed: 12 February 2019).

House of Commons (2015[c]) *Factsheet – Communications Data*. Available at: [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/473747/Factsheet-Communications\\_Data\\_General.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/473747/Factsheet-Communications_Data_General.pdf) (Accessed: 12 February 2019).

House of Commons (2015[d]) *Operational Case for Bulk Powers*. Available at: [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/504187/Operational\\_Case\\_for\\_Bulk\\_Powers.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/504187/Operational_Case_for_Bulk_Powers.pdf) (Accessed: 12 February 2019).

Howard, P.N. and Kollanyi, B. (2016) *Bots, #strongerin, and #brexit: Computational propaganda during the UK-EU referendum*. Available at: <https://arxiv.org/ftp/arxiv/papers/1606/1606.06356.pdf> (Accessed 12 April 2018).

Howard, P.N., Bolsover, G., Kollanyi, B., Bradshaw, S. and Neudert, L.M., (2017) *Junk News and Bots during the US Election: What Were Michigan Voters Sharing Over Twitter?* Available at: <http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/03/What-Were-Michigan-Voters-Sharing-Over-Twitter-v2.pdf> (Accessed: 11 April 2018).

Howard, P.N. and Woolley, S.C. (2016) ‘Political communication, computational propaganda, and autonomous agents-Introduction’, *International Journal of Communication*, 10(2016), pp 4882–4890.

- Hulcoop, A., Scott-Railton, J., Tanchak, P., Brooks, M., and Deibert, R. (2017) *Tainted Leaks Disinformation and Phishing with a Russian Nexus*. Available at: <https://citizenlab.ca/2017/05/tainted-leaks-disinformation-phish/> (Accessed 17 September 2018).
- Human Rights Data Analysis Group (2016) *Guatemala Memory of Silence: Report of the Commission for Historical Clarification Conclusions and Recommendations*. Available at: <https://hrdag.org/wp-content/uploads/2013/01/CEHreport-english.pdf> (Accessed: 2 December 2019)
- Human Rights Watch (2016) *US: Pass USA Freedom Act*. Available at: <https://www.hrw.org/news/2015/04/30/us-pass-usa-freedom-act> (Accessed: 08 December 2019)
- Ibhawoh, B. (2007) 'Second World War propaganda, imperial idealism and anti-colonial nationalism in British West Africa', *Nordic journal of African studies*, 16(2), pp.221-243.
- IBM (2018) *IBM X-Force Threat Intelligence Index 2018*. Available at: <https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=77014377USEN> (Accessed: 25 December 2018).
- Innes, M. (2003) *Understanding social control: Deviance, crime and social order*. Maidenhead: Open University press.
- Intelligence Services Act 1994*, c .13. UK Available at: [http://www.legislation.gov.uk/ukpga/1994/13/pdfs/ukpga\\_19940013\\_en.pdf](http://www.legislation.gov.uk/ukpga/1994/13/pdfs/ukpga_19940013_en.pdf) (Accessed: 13 February 2018).
- International Criminal Court (n.d.[a]) *Understanding the International Criminal Court*. Available at: <https://www.icc-cpi.int/iccdocs/PIDS/publications/UICCEng.pdf> (Accessed: 1 January 2020)

International Criminal Court (n.d.[b]) *How the Court works*. Available at: <https://www.icc-cpi.int/about/how-the-court-works> (Accessed: 1 January 2020).

International Criminal Court (2005) *Darfur, Sudan*. Available at: <https://www.icc-cpi.int/darfur> (Accessed: 1 January 2020)

International Committee of the Red Cross (n.d.) *The Geneva Conventions and their Additional Protocols*. Available at: <https://www.icrc.org/en/war-and-law/treaties-customary-law/geneva-conventions> (Accessed: 22 May 2019).

International Court of Justice (2019) *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*. Available at: <https://www.icj-cij.org/en/case/70> (Accessed: 4 June 2019).

International Monetary Fund, (2019) *The IMF and the World Bank*. Available at: <https://www.imf.org/en/About/Factsheets/Sheets/2016/07/27/15/31/IMF-World-Bank> (Accessed: 19 December 2019)

*Investigatory Powers Act 2016*, c. 25. Available at: [http://www.legislation.gov.uk/ukpga/2016/25/pdfs/ukpga\\_20160025\\_en.pdf](http://www.legislation.gov.uk/ukpga/2016/25/pdfs/ukpga_20160025_en.pdf) (Accessed: 27 April 2018).

Investopedia (2019) *Dark Web*. Available at: <https://www.investopedia.com/terms/d/dark-web.asp> (Accessed: 10 December 2019)

ITV News (2019[a]) *Boris Johnson ordered to court over 2016 Brexit comments: ITV News*. Available at: <https://www.youtube.com/watch?v=ZMrupXIeZo4> (Accessed: 7 November 2019)

ITV News (2019[b]) *Boris Johnson unveils new battle bus as Tory general election campaign hits the road*. Available at: <https://www.itv.com/news/2019-11-15/well-deliver-greener-vehicles-insists-pm-as-he-unveils-battlebus/> (Accessed: 6 December 2019)

- Jackson, R. and Sørensen, G. (2016) *Introduction to International Relations: Theories and approaches*. 6th edn. Oxford: Oxford University Press.
- Jaitner, M.L. (2015) 'Russian Information Warfare: Lessons from Ukraine', in Geers, K. (ed.) *Cyber War in Perspective: Russian Aggression against Ukraine*. Tallinn: NATO CCD COE Publications, Available at: [https://ccdcoe.org/uploads/2018/10/CyberWarinPerspective\\_full\\_book.pdf](https://ccdcoe.org/uploads/2018/10/CyberWarinPerspective_full_book.pdf) (Accessed: 20 December 2019)
- Jensen, R. (2011) 'Pornography as Propaganda', in Sussman, G. (ed.) *The Propaganda society: Promotional Culture and Politics in Global Context*. New York: Peter Lang, pp. 159 – 174.
- Johansson-Nogués, E. (2018) 'The EU's ontological (in) security: Stabilising the ENP area... and the EU-self?', *Cooperation and Conflict*, 00(0), pp. 1-17.
- Joh, E. E. (2016) *The Government Shouldn't Distribute Child Pornography. Period*. Available at: <https://www.nytimes.com/roomfordebate/2016/01/27/the-ethics-of-a-child-pornography-sting/the-government-shouldnt-distribute-child-pornography-period> (Accessed: 10 December 2019).
- John F Kennedy Presidential Library and Museum (n.d.) *Address During The Cuban Missile Crisis*. Available at: <https://www.jfklibrary.org/learn/about-jfk/historic-speeches/address-during-the-cuban-missile-crisis> (Accessed: 1 November 2019)
- Johns Hopkins University (2014) *The Johns Hopkins Foreign Affairs Symposium Presents: The Price of Privacy: Re-Evaluating the NSA*. Available at: <https://www.youtube.com/watch?v=kV2HDM86XgI> (Accessed: 29 September 2018).
- Johnson, L.K., Aldrich, R.J., Moran, C., Barrett, D.M., Hastedt, G., Jervis, R., Krieger, W., McDermott, R., Omand, D., Phythian, M. and Wark, W.K. (2014) 'An INS special

forum: Implications of the Snowden leaks’, *Intelligence and National Security*, 29(6), pp. 793-810.

Johnson, T.J., & Fahmy, S. (2009) ‘Embeds’ Perceptions of Censorship: Can You Criticize a Soldier Then Have Breakfast With Him in the Morning?’, *Mass Communication and Society*, 12:1, 52-77.

Johnson, T.R. (n.d.) *American Cryptology during the Cold War*. Available at: <https://nsarchive2.gwu.edu/NSAEBB/NSAEBB260/nsa-5.pdf> (Accessed: 28 October 2018).

Johnson, R. (2017) *State Secrets: How an Avalanche of Media Leaks is Harming National Security*. Available at: <https://www.hsgac.senate.gov/imo/media/doc/2017-07-06%20State%20Secrets%20report.pdf> (Accessed: 2 January 2019)

Jones, A. (2006) *Dictionary of Globalization*. Cambridge: Polity.

Jones, S. (2017) *Leaked CIA cyber tricks may make us WannaCry some more*. Available at: <https://www.ft.com/content/a7a6c91c-3a35-11e7-ac89-b01cc67cfeec> (Accessed: 20 November 2017).

Jones, S.G. (2018) *Going on the Offensive: A U.S. Strategy to Combat Russian Information Warfare*. Available at: <https://www.csis.org/analysis/going-offensive-us-strategy-combat-russian-information-warfare> (Accessed: 27 November 2018).

Jordan, W. (2015) *S Africa spied on Russia for satellite project details*. Available at: <https://www.aljazeera.com/news/2015/02/south-africa-russia-joint-satellite-project-condor-spy-cables-guardian-150225154536792.html> (Accessed: 15 May 2019).

Jordan, T. and Taylor, P.A. (2004) *Hactivism and Cyberwars: Rebels with a Cause?* London: Routledge.

- Jorgensen, I. (2006) *Timeline: How the cartoon crisis unfolded*. Available at: <https://www.ft.com/content/d30b0c22-96ee-11da-82b7-0000779e2340> (Accessed: 11 May 2019).
- Joseph, G. and Hussain, M. (2018) *FBI Tracked an Activist Involved With Black Lives Matter as They Travelled Across the U.S., Documents Show*. Available at: <https://theintercept.com/2018/03/19/black-lives-matter-fbi-surveillance/> (Accessed: 20 April 2018).
- Joshua 2: 1, Holy Bible. Good News Bible.
- Joshua 6: 21, Holy Bible. Good News Bible.
- Jowett, G.S. and O'Donnell, V. (2011) *Propaganda and Persuasion*. 5th edn. Los Angeles: SAGE Publications.
- Justia (2018) *Jacobson v. United States, 503 U.S. 540 (1992)*. Available at: <https://supreme.justia.com/cases/federal/us/503/540/case.html> (Accessed: 29 June 2018).
- Justia (2019[a]) *Buck v. Bell, 274 U.S. 200 (1927)*. Available at: <https://supreme.justia.com/cases/federal/us/274/200/> (Accessed: 12 November 2019)
- Justia (2019[b]) *Sherman v. United States, 356 U.S. 369 (1958)*. Available at: <https://supreme.justia.com/cases/federal/us/356/369/> (Accessed: 18 December 2019)
- Kamminga, M.R. (2017) 'Cosmopolitan Europe? Cosmopolitan justice against EU-centredness', *Ethics & Global Politics*, 10(1), pp.1-18.
- Kant, I. (1991) *Political Writings*. 2<sup>nd</sup> edn. Translated by Nisbet, H.B. Rev. edn. Cambridge: Cambridge University Press.

Kant, I. (1983) *Perpetual Peace and Other Essays on Politics, History, and Morals*. Translated by Humphrey, T. Rev. edn. Indianapolis: Hackett Publishing Company.

Kaspersky (2019[a]) *What is Cyber-Security?* Available at:

<https://www.kaspersky.co.uk/resource-center/definitions/what-is-cyber-security>  
(Accessed: 29 April 2019).

Kaspersky (2019[b]) *What is a DDoS Attack? - DDoS Meaning*. Available at:

<https://www.kaspersky.co.uk/resource-center/threats/ddos-attacks> (Accessed: 6 May 2019).

Kaspersky, 2019[c]) *Learn about malware and how to protect all your devices against it*.

Available at: <https://www.kaspersky.com/resource-center/preemptive-safety/what-is-malware-and-how-to-protect-against-it> (Accessed: 9 June 2019).

Karatzogianni, A. and Robinson, A. (2017) 'Schizorevolutions versus microfascisms: The fear of anarchy in state securitisation', *Journal of International Political Theory*, 13(3), pp. 282-295.

Karp, A. (2011) *Palantir's technology to fight terrorism*. Available at:

<https://www.palantir.com/wp-assets/wp-content/static/pg-analysis-blog/2011/08/Techscan-Palantir.pdf> (Accessed: 14 November 2019)

Karp, R. (2018) 'Identity and anxiety: Germany's struggle to lead', *European Security*, 27(1), pp. 58-81.

Kaufman, A. A. (2011) *The "Century of Humiliation" and China's National Narratives*.

Available at: <https://www.uscc.gov/sites/default/files/3.10.11Kaufman.pdf> (Accessed: 1 January 2019).

Keiber, J. (2015) 'Surveillance hegemony', *Surveillance & Society*, 13(2), pp.168-181.



- Kelion, L. (2019) *Google wins landmark right to be forgotten case*. Available at: <https://www.bbc.co.uk/news/technology-49808208> (Accessed: 7 December 2019)
- Keohane, R.O. (1986) 'Theory of World Politics: *Structural Realism and Beyond*' in Keohane, R.O. (ed.) *Neorealism and Its Critics*. New York: Colombia University Press, pp. 158 – 203.
- Keohane, R.O. (1990) 'Multilateralism: an agenda for research', *International journal*, 45(4), pp.731-764.
- Keohane, R.O. and Martin, L.L. (1995) 'The promise of institutionalist theory', *International Security*, 20(1), pp.39-51.
- Kellner, D. (2004) 'Media propaganda and spectacle in the war on Iraq: A critique of US broadcasting networks', *Cultural Studies? Critical Methodologies*, 4(3), pp.329-338.
- Kershaw, R. (2015) *Collar the lot! Britain's policy of internment during the Second World War*. Available at: <http://blog.nationalarchives.gov.uk/blog/collar-lot-britains-policy-internment-second-world-war/> (Accessed: 25 April 2018).
- Khanna, A., Pandey, B., Vashishta, K., Kalia, K., Pradeepkumar, B. and Das, T. (2015) 'A study of today's AI through chatbots and rediscovery of machine intelligence', *International Journal of u- and e- Service, Science and Technology* 8(7), pp.277-284.
- 'Kidane v. The Federal Republic of Ethiopia' (2017) United States Court of Appeals, case No. 16-7081. United States Court of Appeals for the District of Columbia Circuit [Online]. Available at: [https://www.cadc.uscourts.gov/internet/opinions.nsf/E0C614D73F037CAD852580E3004EE648/\\$file/16-7081-1665840.pdf](https://www.cadc.uscourts.gov/internet/opinions.nsf/E0C614D73F037CAD852580E3004EE648/$file/16-7081-1665840.pdf) (Accessed: 28 September 2018).

- King, G., Pan, J. and Roberts, M.E. (2013) 'How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument', *American Political Science Review*, 111(3), pp. 484–501.
- Kinnvall, C. (2017) 'Feeling ontologically (in) secure: States, traumas and the governing of gendered space', *Cooperation and Conflict*, 52(1), pp. 90-108.
- Kinnvall, C. and Mitzen, J. (2017) 'An introduction to the special issue: Ontological securities in world politics', *Cooperation and Conflict*, 52(1), pp. 3-11.
- Kimble, C. E. (1990) *Social Psychology: Studying Human Interaction*. Dubuque: Wm.C. Brown Publishers.
- Koskenniemi, M. (2011) *The politics of international law*. Oxford : Hart Publishing.
- Klaas, B. (2016) *The Despot's Accomplice: How the West is Aiding and Abetting the Decline of Democracy*. London: C. Hurst & Co.
- Klautke, E. (2016) "'The Germans are beating us at our own game' American eugenics and the German sterilization law of 1933", *History of the Human Sciences*, 29(3), pp.25-43.
- Koppang, H. (2009) 'Social Influence by Manipulation: A Definition and Case of Propaganda', *Middle East Critique*, 18(2), pp. 117-143.
- Kremling, J. and Parker, A. M. S. (2018) *Cyberspace, Cybersecurity, and Cybercrime*. Los Angeles: SAGE.
- Kroger, C.A. (2011) *ELINT: A Scientific System*. Available at: [https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol2no1/html/v02i1a06p\\_0001.htm](https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol2no1/html/v02i1a06p_0001.htm) (Accessed: 24 April 2018).

- Kumar, D (2006) 'Media, War, and Propaganda: Strategies of Information Management During the 2003 Iraq War', *Communication and Critical/Cultural Studies*, 3(1), 48-69.
- Kumar, S. (2018) 'Untying the Mystique of an Islamic Threat: Western Imageries, the Clash of Civilizations, and a Search for Ontological Security', *Jadavpur Journal of International Relations*, 22(1), pp.1-21.
- Kux, D. (1985) 'Soviet active measures and disinformation: overview and assessment', *Parameters, Journal of the US Army War College*, 15(4), pp.19 -28. Available at: <http://ssi.armywarcollege.edu/pubs/parameters/Articles/1985/1985%20kux.pdf> (Accessed: 23 September 2018).
- Laing, D. (1965) *The Divided Self An existential study in sanity and madness*. Harmondsworth: Penguin Books.
- Langston, J. (2017) *Lip-syncing Obama: New tools turn audio clips into realistic video*. Available at: <https://www.washington.edu/news/2017/07/11/lip-syncing-obama-new-tools-turn-audio-clips-into-realistic-video/> (Accessed: 24 May 2019).
- Lapowsky, I. (2018) *Facebook Exposed 87 Million Users to Cambridge Analytica*. Available at: <https://www.wired.com/story/facebook-exposed-87-million-users-to-cambridge-analytica/> (Accessed: 14 November 2019)
- Larsson, G. and Lindekilde, L. (2009) 'Muslim claims-making in context: Comparing the Danish and the Swedish Muhammad cartoons controversies', *Ethnicities*, 9(3), pp.361-382.
- Lasswell, H.D. (1927) 'The theory of political propaganda', *American Political Science Review*, 21(3), pp. 627-631.
- Laswell, H.D. (1972) *Propaganda Technique in the World War*. London: Garland.

Lasswell, H.D. (1935) 'The person: Subject and object of propaganda', *The ANNALS of the American Academy of Political and Social Science*, 179(1), pp. 187-193.

Le Bon, G. (2014) *The Crowd, study of the popular mind*. USA: Aristeus Books.

Lechner, S. (2017) 'Why anarchy still matters for International Relations: On theories and things', *Journal of International Political Theory*, 13(3), pp. 341-359.

Legatum Institute (2014) *The Menace of Unreality: Combatting Russian Disinformation in the 21st Century*. Available at: [https://www.youtube.com/watch?time\\_continue=4&v=KwZZFuuiQ2I&feature=emb\\_logo](https://www.youtube.com/watch?time_continue=4&v=KwZZFuuiQ2I&feature=emb_logo) (Accessed: 2 January 2020)

Lee, M. Y. H. (2015) *Donald Trump's false comments connecting Mexican immigrants and crime*. Available at: <https://www.washingtonpost.com/news/fact-checker/wp/2015/07/08/donald-trumps-false-comments-connecting-mexican-immigrants-and-crime/> (Accessed: 6 November 2019)

Leiss, W. and Chociolko, C. (1994) *Risk and Responsibility*. Montreal: McGill-Queens University Press.

Leitenberg, M. (2016) *China's False Allegations of the Use of Biological Weapons by the United States during the Korean War*. Available at: <https://www.wilsoncenter.org/publication/chinas-false-allegations-the-use-biological-weapons-the-united-states-during-the-korean> (Accessed: 8 April 2019).

LePage, J-M. (2010) *The Battle for Hearts and Minds: Counterinsurgency and Reconstruction Programs in Vietnam*. Available at: <https://history.state.gov/conferences/2010-southeast-asia/battle-for-hearts-and-minds> (Accessed: 17 May 2020)

Levite, A.E. and Jinghua, L. (2019) *Chinese-American Relations in Cyberspace: Toward Collaboration or Confrontation?* China Military Science. Available at:

<https://carnegieendowment.org/2019/01/24/chinese-american-relations-in-cyberspace-toward-collaboration-or-confrontation-pub-78213> (Accessed: 2 January 2020)

Lewis, J. A. (2015) *UN publishes latest Report of the Group of Government Experts*. Available at: <https://www.csis.org/blogs/strategic-technologies-blog/un-publishes-latest-report-group-government-experts> (Accessed: 20 December 2017).

Lewis, L. and Vavrichek, D.M. (2016) *Rethinking the Drone War: National Security, Legitimacy, and Civilian Casualties in U.S. Counterterrorism Operations*. Virginia: Marine Corps University Press and CNA Corporation.

Lewis, P. Pegg, D. and Hern. A. (2018) *Cambridge Analytica kept Facebook data models through US election*. Available at: <https://www.theguardian.com/uk-news/2018/may/06/cambridge-analytica-kept-facebook-data-models-through-us-election> (Accessed: 2 April 2019).

Liberal Democrats (2017) *Theresa May defends '£350million for NHS' Vote Leave claim*. Available at: <https://www.youtube.com/watch?v=8HbO21sD7EQ> (Accessed: 7 November 2019)

Liberty (2018) *Court of Appeal rules Government surveillance regime IS unlawful*. Available at: <https://www.libertyhumanrights.org.uk/news/press-releases-and-statements/court-appeal-rules-government-surveillance-regime-unlawful> (Accessed: 20 December 2018).

Liberty, (2019) *MI5 "UNLAWFULLY" Handled Bulk Surveillance Data, Liberty Litigation Reveals*. Available at: <https://www.libertyhumanrights.org.uk/news/press-releases-and-statements/mi5-%E2%80%9Cunlawfully%E2%80%9D-handled-bulk-surveillance-data-liberty> (Accessed: 3 November 2019).

Library of Congress (1932) *Sorrells v United States*. Available at: <http://cdn.loc.gov/service/ll/usrep/usrep287/usrep287435/usrep287435.pdf> (Accessed: 2 January 2020)

Library of Congress (1941) *Speech by Franklin D. Roosevelt, New York (Transcript)*. Available at: [https://www.loc.gov/resource/afc1986022.afc1986022\\_ms2201/?st=text](https://www.loc.gov/resource/afc1986022.afc1986022_ms2201/?st=text) (Accessed: 21 May 2019).

Library of Congress (1985) *Hearings Before the Subcommittee On European Affairs Of the committee On Foreign Relations United States Senate Ninety-Ninth Congress First Session On United States Policy Toward East Europe, West Europe, and the Soviet Union*. Available at: [http://www.loc.gov/law/find/nominations/gates/017\\_excerpt.pdf](http://www.loc.gov/law/find/nominations/gates/017_excerpt.pdf) (Accessed: 10 December 2017).

Library of Congress (2015) *"Suffering Under a Great Injustice": Ansel Adams's Photographs of Japanese-American Internment at Manzanar*. Available at: <http://www.loc.gov/teachers/classroommaterials/connections/manzanar/history2.html> (Accessed: 25 April 2018).

Lim, G., Maynier, E., Scott-Railton, J., Fittarelli, A., Moran, N and Deibert, R. (2019) *Burned After Reading: Endless Mayfly's Ephemeral Disinformation Campaign*. Available at: <https://citizenlab.ca/2019/05/burned-after-reading-endless-mayflys-ephemeral-disinformation-campaign/> (Accessed: 24 May 2019).

Lim, Y.J. and Lemanski, J.L. (2017) 'Psychological Words in Music and Propagandistic Communication in Two Koreas over the DMZ', *Journal of Creative Communications*, 12(3), pp.159-170.

Lippmann, W. (1993) *The Phantom Public*. In McClay, W. M. Rev. edn. London: Transaction Publishers.

Lippmann, L. (1997) *Public Opinion*. Rev. edn. New York: Free Press PaperBacks

Logan, S. (2017) 'The needle and the damage done: Of haystacks and anxious panopticons', *Big Data & Society*, 4(2), pp. 1-13.

- Lopez, E. E. (2013) *Jorge Rafael Videla, Jailed Argentine Military Leader, Dies at 87*. Available at: <https://www.nytimes.com/2013/05/18/world/americas/jorge-rafael-videla-argentina-military-leader-in-dirty-war-dies-at-87.html> (Accessed: 3 November 2019)
- Louw, P.E. (2005) *The Media And Political Process*. London: Sage.
- Lovell, J (2012) *The Opium War*. London: Picador.
- Lucas, E. and Pomeranzev, p. (2016) *Winning the Information War. Techniques and Counter-strategies to Russian Propaganda in Central and Eastern Europe*. Available at: <https://lif.blob.core.windows.net/lif/docs/default-source/publications/winning-the-information-war-full-report-pdf?sfvrsn=2> (Accessed: 25 October 2018).
- Luhn, A. (2015) *US gives Russian newspaper grammar lesson over 'fake letter' to LGBT activist*. Available at: <https://www.theguardian.com/world/2015/nov/19/us-embassy-russian-newspaper-grammar-lesson-fake-letter-lgbt-activist-nikolai-alexeyev> (Accessed: 3 June 2018).
- Luke 20:19-25, Holy Bible. Good News Bible.
- Lyon, D. (1994) *The Electronic Eye The Rise Of Surveillance Society*. Cambridge: Polity Press.
- Lyon, D. (2006) 'The search for surveillance theories' in Lyon, D. (ed.) *Theorizing Surveillance: The panopticon and beyond*. Devon: Willian Publishing, pp. 3-20.
- Lyon, D. (2012) *Surveillance society: Monitoring everyday life*. Buckingham: Open University.
- Lyon, D (2014[a]) 'Surveillance and the Eye of God', *Studies in Christian Ethics*, 27(1), pp. 21-32.

- Lyon, D. (2014[b]) 'Surveillance, Snowden, and big data: Capacities, consequences, critique', *Big Data & Society*, 1(2), pp. 1-13.
- Lyon, D. (2015) 'The Snowden stakes: challenges for understanding surveillance today', *Surveillance & Society*, 13(2), pp. 139-152.
- MacFarquhar, N. (2016) *A Powerful Russian Weapon: The Spread of False Stories*. Available at: <https://www.nytimes.com/2016/08/29/world/europe/russia-sweden-disinformation.html> (Accessed: 17 September 2018).
- Machiavelli, N. (1988) *The Prince*, in Skinner, Q. and Price, R. (ed.). Rev. edn. Cambridge: Cambridge University Press.
- Maclean, R. (2017) *British PR firm Bell Pottinger apologizes for South Africa campaign*. Available at: <https://www.theguardian.com/uk-news/2017/jul/10/bell-pottinger-pr-firm-apologizes-south-africa-campaign> (Accessed: 20 November 2019)
- Madley, B. (2005) 'From Africa to Auschwitz: How German South West Africa incubated ideas and methods adopted and developed by the Nazis in Eastern Europe', *European History Quarterly*, 35(3), pp.429-464.
- MAG (n.d.[a]) *What we do*. Available at: <https://www.maginternational.org/what-we-do/> (Accessed: 31 December 2018).
- MAG (n.d.[b]) *Laos*. Available at: <https://www.maginternational.org/what-we-do/where-we-work/laos/> (Accessed: 31 December 2018).
- Mann, S. and Ferenbok, J. (2013) 'New media and the power politics of sousveillance in a surveillance-dominated world', *Surveillance & Society*, 11(1/2), pp. 18-34.



- Mann, S., Nolan, J. and Wellman, B. (2003) 'Sousveillance: Inventing and using wearable computing devices for data collection in surveillance environments', *Surveillance & society*, 1(3), pp.331-355.
- Markham, T. (2014) 'Social media, protest cultures and political subjectivities of the Arab spring', *Media, Culture & Society*, 36(1), pp.89-104.
- Martha, A, Iain, W. and Donaghue, N. (2014) *Social Cognition : An Integrated Introduction*. Los Angeles: SAGE
- Mathew 22:37-40, Holy Bible. Good News Bible.
- Martin, L.J. (1971) 'Effectiveness of international propaganda', *The ANNALS of the American Academy of Political and Social Science*, 398(1), pp. 61-70.
- Masaharu, S (1999) 'Negro Propaganda Operations': Japan's short-wave radio broadcasts for World War II Black Americans', *Historical Journal of Film, Radio and Television*, 19(1), 5-26.
- Masco, J. (2017) 'Boundless informant': Insecurity in the age of ubiquitous surveillance', *Anthropological Theory*, 17(3), pp. 382-403.
- Maass, M. (2009) 'Catalyst for the Roosevelt Corollary: Arbitrating the 1902–1903 Venezuela Crisis and Its Impact on the Development of the Roosevelt Corollary to the Monroe Doctrine', *Diplomacy & Statecraft*, 20(3), pp.383-402.
- Mastanduno, M. (1999) 'A Realist view: three images of the coming international order', in Paul, T.V. and Hall, J.A (ed.). *International Order and the Future of World Politics*. Cambridge: Cambridge University Press, pp. 19-40.

- Matei, F.C. and Bruneau, T.C. (2011) 'Policymakers and Intelligence Reform in the New Democracies', *International Journal of Intelligence and CounterIntelligence*, 24(4), pp. 656-691.
- Matei, F.C. (2014) 'The media's role in intelligence democratization', *International Journal of Intelligence and CounterIntelligence*, 27(1), pp. 73-108.
- May, T. (2011) *Social Research: Issues, Methods and Process*. 4<sup>th</sup> edn. Maidenhead: Open University Press.
- Mazetti, M. and Daragahi, B. (2005) *U.S. Military Covertly Pays to Run Stories in Iraqi Press*. Available at: <https://www.latimes.com/archives/la-xpm-2005-nov-30-fg-infowar30-story.html> (Accessed at: 13 December 2019)
- McAdams, R.H. (2007) 'Reforming Entrapment Doctrine in United States v. Hollingsworth', *University of Chicago Law Review*, 74, p.1795-1812.
- McCarthy, N (2017) *Norway's Sovereign Wealth Fund Hits \$1 Trillion [Infographic]*. Available at: <https://www.forbes.com/sites/niallmccarthy/2017/09/22/norways-sovereign-wealth-fund-hits-1-trillion-infographic/#5bd4e28f83c9> (Accessed: 1 January 2019).
- McClintok, B. (2017) *Russian Information Warfare: A Reality That Needs a Response*. Available at: <https://www.rand.org/blog/2017/07/russian-information-warfare-a-reality-that-needs-a.html> (Accessed: 25 October 2018)
- McCoy, A. (2015) 'Policing the imperial periphery: The Philippine-American War and the origins of US Global Surveillance', *Surveillance & Society*, 13(1), pp. 4- 26.
- McDonald, R. A. and Moreno, S. K. (2005) *Raising the Periscope... Grab and Poppy: America's Early ELINT Satellites*. Available at:

<http://www.nro.gov/Portals/65/documents/history/csnr/programs/docs/prog-hist-03.pdf>  
(Accessed: 2 November 2018).

- McGreal, C. (2010) *Wikileaks reveals video showing US air crew shooting down Iraqi civilians*. Available at: <https://www.theguardian.com/world/2010/apr/05/wikileaks-us-army-iraq-attack> (Accessed: 6 May 2019).
- McLaughlin, E. (2019) 'State Crime', in McLaughlin, E. and Muncie, J. (eds.) *The Sage Dictionary of Criminology*. 4<sup>th</sup> edn. Los Angeles: SAGE, pp. 522 – 523.
- McKinlay, A., Carter, C. and Pezet, E. (2012) 'Governmentality, power and organization', *Management & Organizational History*, 7(1), pp.3-15.
- McKnight, D. (2008) 'Not Attributable to Official Sources': Counter-Propaganda and the Mass Media', *Media International Australia*, 128(1), pp.5-17.
- McLaren, P. and Martin, G. (2004) 'The legend of the Bush gang: Imperialism, war, and propaganda', *Cultural Studies? Critical Methodologies*, 4(3), pp.281-303.
- McStay, A. (2014) *Privacy and Philosophy*. New York: Peter Lang.
- Mearsheimer, J.J. (1994) 'The false promise of international institutions', *International security*, 19(3), pp. 5-49.
- Mearsheimer, J.J. (2013) 'Structural Realism' in Dunne, T, Kurki, M and Smith, S (ed.) *International Relations Theories: Discipline and Diversity*. 3<sup>rd</sup> edn. Oxford: Oxford University Press, pp. 71-88.
- Medium (2016) *Everything we know of NSA and Five Eyes malware*. Available at: <https://medium.com/@botherder/everything-we-know-of-nsa-and-five-eyes-malware-e8eac172d3b5> (Accessed 14: February 2018).

Medium (2017) *Fakes, Bots, and Blockings in Armenia*. Available at:

<https://medium.com/dfirlab/fakes-bots-and-blockings-in-armenia-44a4c87ebc46>

(Accessed: 28 June 2018).

Melman, Y. (2007) Shin Bet Chief Who Handed Famed Khrushchev Speech to CIA Dies at 88.

Available at: <https://www.haaretz.com/1.4959300> (Accessed: 4 November 2019)

Mendieta, E. (2009) 'From imperial to dialogical cosmopolitanism' *Ethics & Global*

*Politics*, 2(3), pp.241-258.

Menn, J. (2017) *Distrustful U.S. allies force spy agency to back down in encryption fight*.

Available at: <https://www.reuters.com/article/us-cyber-standards-insight/distrustful-u-s-allies-force-spy-agency-to-back-down-in-encryption-fight-idUSKCN1BW0GV>

(Accessed: 12 February 2018).

Meriam–Webster (2019) Definition of dirty tricks. Available at: <https://www.merriam-webster.com/dictionary/dirty%20tricks>

(Accessed: 16 April 2019).

MI5 (n.d.[a]) *Cyber*. Available at: <https://www.mi5.gov.uk/fa/cyber> (Accessed: 23 December

2018).

MI5 (n.d.[b]) *Espionage*. Available at: <https://www.mi5.gov.uk/fa/espionage> (Accessed: 23

December 2018).

MI5 (n.d.[c]) *How Spies Operate*. Available at: <https://www.mi5.gov.uk/how-spies-operate>

(Accessed: 23 December 2018).

MI5 (n.d.[d]) *Equipment Interference*. Available at: <https://www.mi5.gov.uk/fa/node/447>

(Accessed: 23 December 2018).

MI5 (n.d.[e]) *Law and Governance*. Available at: <https://www.mi5.gov.uk/law-and-governance>

(Accessed: 19 August 2018).

- Middle East Eye (2018) *Middle East leaders back Saudi Arabia after Jamal Khashoggi's disappearance*. Available at: <https://www.middleeasteye.net/news/jamal-khashoggi-what-arab-leaders-have-said-about-journalists-disappearance-736661559> (Accessed: 28 November 2018).
- Michael, M. (2019) *Sudan army removes leader, rejects al-Bashir extradition*. Available at: <https://apnews.com/47f23657c32b4c3c9c22c7c2bb174b51> (Accessed: 1 January 2019)
- Mill, J. S. (1992) *On Liberty and Utilitarianism*. London: David Campbell Publishers.
- Milne, S. and MacAskill, E. (2015) *South Africa spied on own government to get facts on joint project with Russia*. Available at: <https://www.theguardian.com/world/2015/feb/25/south-africa-spied-government-facts-joint-russian-project> (Accessed: 2 May 2017).
- Miller, C. (2005) 'Introduction', in Bernays, E. (ed.) *Propaganda*. New York: Ig Publishing, pp. 9-33.
- Miller, D. (2004) 'The Propaganda Machine' in Miller, D. (ed.) *Tell me lies Propaganda and Media Distortion in the Attack on Iraq*. London: Pluto, pp 89 -90.
- Ministry of the Armed Forces (France), (2019) *IndoChina*. Available at: <https://www.defense.gouv.fr/english/dgse/tout-le-site/indochina> (Accessed: 17 May 2020)
- Ministry Of Defence (UK) (2013) *Joint Doctrine Note 2/13 Information Superiority*. Available at: [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/239342/20130813\\_JDN\\_2\\_13\\_Info\\_Super.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/239342/20130813_JDN_2_13_Info_Super.pdf) (Accessed: 25 April 2018).

Ministry of Defence (UK) (2015) *Allied joint doctrine for psychological operations (AJP-3.10.1)*. Available at:

[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/450521/20150223-AJP\\_3\\_10\\_1\\_PSYOPS\\_with\\_UK\\_Green\\_pages.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/450521/20150223-AJP_3_10_1_PSYOPS_with_UK_Green_pages.pdf)

(Accessed: 6 May 2019).

Ministry of Defence (2016) *Cyber Primer*. Available at:

[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/549291/20160720-Cyber\\_Primer\\_ed\\_2\\_secured.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/549291/20160720-Cyber_Primer_ed_2_secured.pdf) (Accessed: 25 December

2018).

Ministry of Defence and Fallon, M. (2017) *British soldiers arrive in Estonia*. Available at:

<https://www.gov.uk/government/news/british-soldiers-arrive-in-estonia> (Accessed: 12

February 2019).

Ministry of Foreign Affairs Russia, (2018) *Sincere thanks to Mrs May for #HighlyLikelyRussia*

*It's gone to people... And here is the first news for #HighlyLikelyRussia*. [Twitter] 12

March. Available at: <https://twitter.com/search?q=%23HighlyLikelyRussia> (Accessed:

22 November 2019)

Mitzen, J. (2006) 'Ontological security in world politics: State identity and the security dilemma', *European Journal of international relations*, 12(3), pp. 341-370.

Moran, C. (2011) 'Intelligence and the Media: The Press, Government Secrecy and the 'Buster' Crabb Affair', *Intelligence and National Security*, 26(5), pp. 676-700.

Morin, R. (2018) *White House targets Iran with new counterterrorism strategy*. Available at:

<https://www.politico.com/story/2018/10/04/white-house-iran-strategy-869511>

(Accessed: 29 April 2019).

Munholland, J.K. (1981) 'Collaboration Strategy' and the French Pacification of Tonkin, 1885–1897', *The Historical Journal*, 24(3), pp.629-650.

- Munoz, A. (2012) *U.S. Military Information Operations in Afghanistan: Effectiveness of Psychological Operations 2001–2010*. Available at: [https://www.rand.org/content/dam/rand/pubs/monographs/2012/RAND\\_MG1060.pdf](https://www.rand.org/content/dam/rand/pubs/monographs/2012/RAND_MG1060.pdf) (Accessed: 6 May 2019).
- Murphy, M.H. (2014) ‘The pendulum effect: comparisons between the Snowden revelations and the Church Committee. What are the potential implications for Europe?’, *Information & Communications Technology Law*, 23(3), pp. 192-219.
- Myers, D., Abell, J., Kolstad, A. and Sani, F. (2010) *Social Psychology*. European Edition. Maidenhead: McGraw-Hill.
- NBC NEWS (2014[a]) *Exclusive: Snowden Docs Show UK Spies Attacked Anonymous, Hackers*. Available at: <https://www.nbcnews.com/feature/edward-snowden-interview/exclusive-snowden-docs-show-uk-spies-attacked-anonymous-hackers-n21361> (Accessed: 6 March 2019).
- NBC NEWS (2014[b]) *No LOL Matter: FBI Trolls Social Media for Would-Be Jihadis*. Available at: <https://www.nbcnews.com/storyline/isis-terror/no-lol-matter-fbi-trolls-social-media-would-be-jihadis-n226841> (Accessed: 29 September 2018)
- NBC News (2017) *Who Planted the Fake News at Center of Qatar Crisis?* Available at: <https://www.nbcnews.com/news/world/who-planted-fake-news-center-qatar-crisis-n784056> (Accessed: 2 June 2018).
- Nakashima, E. and Harris, S. (2018) *How the Russians hacked the DNC and passed its emails to WikiLeaks*. Available at: [https://www.washingtonpost.com/world/national-security/how-the-russians-hacked-the-dnc-and-passed-its-emails-to-wikileaks/2018/07/13/af19a828-86c3-11e8-8553-a3ce89036c78\\_story.html?utm\\_term=.00bad369b3fb](https://www.washingtonpost.com/world/national-security/how-the-russians-hacked-the-dnc-and-passed-its-emails-to-wikileaks/2018/07/13/af19a828-86c3-11e8-8553-a3ce89036c78_story.html?utm_term=.00bad369b3fb) (Accessed: 1 March 2019).

National Archives and Records Administration (US) (2016) *Findings on MLK Assassination*.

Available at: <https://www.archives.gov/research/jfk/select-committee-report/part-2e.html#hoover> (Accessed: 3 January 2017).

National Archives and Records of Administration (US) (2017[a]) *Forty Years Ago: The Cuban Missile Crisis*. Available at:

<https://www.archives.gov/publications/prologue/2002/fall/cuban-missiles.html>

(Accessed: 1 November 2019)

National Archives and Records Administration (US) (2017[b]) “*Three Generations of Imbeciles are Enough*” — *The Case of Buck v. Bell*. Available at:

<https://education.blogs.archives.gov/2017/05/02/buck-v-bell/> (Accessed: 12 November 2019)

National Archives and Records Administration (US) (2019) *Fred Hampton*. Available at:

<https://www.archives.gov/research/african-americans/individuals/fred-hampton>

(Accessed: 17 April 2019).

National Audit Office (UK) (2018) *Investigation: WannaCry cyber attack and the NHS*.

Available at: <https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf> (Accessed: 24 October 2018).

National Cyber Security Center (UK) (2018[a]) *Russian military ‘almost certainly’ responsible for destructive 2017 cyber attack*. Available at: <https://www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017-cyber-attack>

(Accessed: 18 November 2018).

National Cyber Security Centre (2018[b]) *Pioneering programme defends UK from millions of cyber attacks*. Available at: <https://www.ncsc.gov.uk/news/pioneering-programme-defends-uk-millions-cyber-attacks>

(Accessed: 25 December 2018).



National Cyber Security Center (2018[c]) *Reckless campaign of cyber attacks by Russian military intelligence service exposed*. Available at:

<https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed> (Accessed: 1 March 2019).

National Geospatial-Intelligence Agency (n.d.[a]) *CORONA Program*. Available at:

<https://www.nga.mil/About/History/NGAinHistory/Pages/CORONAProgram.aspx>  
(Accessed: 24 April 2018). [a]

National Geospatial-Intelligence Agency (n.d.[b]) *A-12 OXCART Reconnaissance Aircraft*.

Available at: <https://www.nga.mil/About/History/NGAinHistory/Pages/OXCART.aspx>  
(Accessed: 1 November 2019)

National Geospatial-Intelligence Agency (n.d.[c]) *Discovery of Soviet Missiles in Cuba*.

Available at:

<https://www.nga.mil/About/History/NGAinHistory/Pages/DiscoveryofSovietMissilesinCuba.aspx> (Accessed: 1 November 2019)

National Museum of the US Air Force (2015) *Igloo White*. Available at:

<https://www.nationalmuseum.af.mil/Visit/Museum-Exhibits/Fact-Sheets/Display/Article/195948/igloo-white/> (Accessed: 2 February 2019).

National Reconnaissance Office (2005) *POPPY Satellite Reconnaissance Program Recognized*.

Available at: <http://www.nro.gov/Portals/65/documents/news/press/2005/2005-06.pdf>  
(Accessed: 24 April 2018).

National Security Agency (n.d.[a]) *Signals Intelligence*. Available at:

<https://www.nsa.gov/what-we-do/signals-intelligence/> (Accessed: 22 December 2018).

National Security Agency (n.d.[b]) *The Zimmerman Telegram*. Available at:

[https://www.nsa.gov/news-features/decclassified-documents/cryptologic-quarterly/assets/files/the\\_zimmermann\\_telegram.pdf](https://www.nsa.gov/news-features/decclassified-documents/cryptologic-quarterly/assets/files/the_zimmermann_telegram.pdf) (Accessed: 25 April 2018).

National Security Agency (n.d.[c]) *Remembrances of VENONA by Mr. William P. Crowell*. Available at: <https://www.nsa.gov/news-features/decclassified-documents/venona/remembrances.shtml> (Accessed: 23rd April 2018).

National Security Archive (US), (n.d.[d]) *Venona Chronology*. Available at: <https://www.nsa.gov/news-features/decclassified-documents/venona/chronology.shtml> (Accessed: 23rd April 2018).

National Security Archive (US), (1953[a]) *Document No. 74: NSC NSC 158, "United States Objectives and Action Plans to Exploit the Unrest in the Satellite States," 29 JUNE 1953*. Available at: <http://nsarchive.gwu.edu/NSAEBB/NSAEBB50/doc74.pdf> (Accessed: 11 July 2018).

National Security Archive (US), (1953[b]) *Document No.38: Psychological Strategy Board Memorandum from John M. Anspacher to George A. Morgan, 17 June 1953*. Available at: <https://nsarchive2.gwu.edu/NSAEBB/NSAEBB50/doc38.pdf> (Accessed: 11 July 2018).

National Security Archive (US), (1976[a]) *CIA cable, "The Role of the National Intelligence Center Within the Countersubversive Campaign," Secret, November 19, 1976*. Available at: <https://nsarchive2.gwu.edu/dc.html?doc=6020961-National-Security-Archive-Doc-12-CIA-cable-The> (Accessed: 2 January 2020)

National Security Archive (US), (1976[b]) *CIA cable, "Argentina: Criticism [over] soft policy toward subversion," Secret, December 3, 1976*. Available at: <https://nsarchive2.gwu.edu/dc.html?doc=5817668-National-Security-Archive-Doc-07-CIA-cable> (Accessed: 30 November 2019).

National Security Archive (US), (2004) *Kissinger to the Argentine Generals in 1976: "If There Are Things To Be Done, You Should Do Them Quickly"*. Available at: <https://nsarchive2.gwu.edu/NSAEBB/NSAEBB133/index.htm> (Accessed: 3 November 2019)

- National Security Archive (US), (2005) *Tonkin Gulf Intelligence "Skewed" According to Official History and Intercepts*. Available at:  
<https://nsarchive2.gwu.edu//NSAEABB/NSAEABB132/press20051201.htm> (Accessed: 20 February 2018).
- National Security Archive (US), (2006[a]) *LITEMPO: The CIA's Eyes on Tlatelolco: CIA Spy Operations in Mexico*. Available at:  
<https://nsarchive2.gwu.edu/NSAEABB/NSAEABB204/index.htm> (Accessed: 26 April 2020)
- National Security Archive (US), (2006[b]) *Information Operations Roadmap*. Available at:  
[https://nsarchive2.gwu.edu/NSAEABB/NSAEABB177/info\\_ops\\_roadmap.pdf](https://nsarchive2.gwu.edu/NSAEABB/NSAEABB177/info_ops_roadmap.pdf) (Accessed: 14 February 2017).
- National Security Archive (US), (2012) *The SOLO File: Declassified Documents Detail "The FBI's Most Valued Secret Agents of the Cold War"*. Available at:  
<https://nsarchive2.gwu.edu/NSAEABB/NSAEABB375/> (Accessed: 26 April 2018).
- National Security Archive (US), (2013) *CIA Confirms Role in 1953 Iran Coup Documents Provide New Details on Mosaddeq Overthrow and Its Aftermath National Security Archive Calls for Release of Remaining Classified Record*. Available at:  
<http://nsarchive.gwu.edu/NSAEABB/NSAEABB435/> (Accessed: 24 April 2017).
- National Security Archive (US), (2015) *Operation Condor: National Security Archive Presents Trove of Declassified Documentation in Historic Trial in Argentina*. Available at:  
<http://nsarchive.gwu.edu/NSAEABB/NSAEABB514/> (Accessed: 20 April 2017).
- National Security Archive (US), (2017) *CIA and Assassinations: The Guatemala 1954 Documents*. Available at: <https://nsarchive2.gwu.edu/NSAEABB/NSAEABB4/index.html> (Accessed: 16 May 2018).

- National Security Archive (US), (2018) *Joint Chiefs of Staff Chairman Maxwell Taylor to Generals LeMay, Wheeler, and Greene, and Admiral McDonald, "Review of the SLOP Guidance," 5 June 1964, CM [Chairman's Memorandum] -1407-64, Top Secret.* Available at: <https://nsarchive2.gwu.edu//dc.html?doc=4775205-Document-02-Joint-Chiefs-of-Staff-Chairman> (Accessed: 31 December 2018).
- NATO Review magazine (2015) *The Paris attacks. A case of intelligence failure?* Available at: <http://www.nato.int/docu/review/2015/ISIS/Paris-attacks-terrorism-intelligence-ISIS/EN/index.htm> (Accessed: 20 April 2017).
- NATO Strategic Communications Centre of Excellence (2018) *Robotrolling: Trump, NATO, and Russian Trolls.* Available at: <https://www.stratcomcoe.org/robotrolling-trump-nato-and-russian-trolls> (2 March 2019).
- NATO Strategic Communications Centre of Excellence (2020) *About us.* Available at: <https://www.stratcomcoe.org/about-us> (Accessed: 19 April 2020)
- Naval History and Heritage Command (2015) *Boxer Rebellion & the US Navy, 1900-1901.* Available at: <https://www.history.navy.mil/content/history/nhhc/research/library/online-reading-room/title-list-alphabetically/b/boxer-rebellion-usnavy-1900-1901.html> (Accessed: 16 December 2018).
- Neudert, L-M., Kollanyi, B and Howard, P.N. (2017) *Junk News and Bots during the German Parliamentary Election: What are German Voters Sharing over Twitter?* Available at: [https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2017/09/ComProp\\_GermanElections\\_Sep2017v5.pdf](https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2017/09/ComProp_GermanElections_Sep2017v5.pdf) (Accessed: 28 April 2019).
- Newburger, E. (2019) *Warren trolls Facebook election ad policy with a 'false' ad that says company endorsed Trump.* Available at: <https://www.cnbc.com/2019/10/12/warren-trolls-facebook-with-false-ad-saying-company-endorsed-trump.html> (Accessed: 14 November 2019)

New York Times (2018) *I Am Part of the Resistance Inside the Trump Administration*.

Available at: <https://www.nytimes.com/2018/09/05/opinion/trump-white-house-anonymous-resistance.html> (Accessed: 30 November 2018).

New Zealand Herald, (2015) *Leaked papers reveal NZ plan to spy on China for US*. Available

at: [https://www.nzherald.co.nz/nz/news/article.cfm?c\\_id=1&objectid=11434886](https://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11434886)  
(Accessed: 18 December 2019)

New Zealand History (n.d.) *Malayan Emergency*. Available at:

<https://nzhistory.govt.nz/war/the-malayan-emergency> (Accessed: 25 April 2020).

North Atlantic Treaty Organisation (1952) *Information Policy Working Group: Positive Information Policy Towards Peoples of NATO Countries: Note By the United Kingdom*

*Delegation*. Available at: [http://archives.nato.int/uploads/r/null/9/1/9133/AC\\_24-D\\_7\\_ENG.pdf](http://archives.nato.int/uploads/r/null/9/1/9133/AC_24-D_7_ENG.pdf) (Accessed 25 May 2019).

North Atlantic Treaty Organisation (1953) *Information Policy Working Group Divisive Propaganda and the Atlantic Alliance*. Available at:

[http://archives.nato.int/uploads/r/null/9/4/9435/AC\\_24-D\\_35\\_ENG.pdf](http://archives.nato.int/uploads/r/null/9/4/9435/AC_24-D_35_ENG.pdf) (Accessed: 25 May 2019).

North Atlantic Treaty Organisation (2018[a]) *Collective defence - Article 5*. Available at:

[https://www.nato.int/cps/en/natohq/topics\\_110496.htm](https://www.nato.int/cps/en/natohq/topics_110496.htm) (Accessed: 16 December 2018).

North Atlantic Treaty Organization (2018[b]) *Speech by NATO Secretary General Jens*

*Stoltenberg at the Cyber Defence Pledge Conference (Ecole militaire, Paris)*. Available at: [https://www.nato.int/cps/en/natohq/opinions\\_154462.htm](https://www.nato.int/cps/en/natohq/opinions_154462.htm) (Accessed: 16 December 2018).

NowThis [@nowthisnews] (2017) *One year ago, we all learned exactly how much respect*

*Donald 'Grab Em By The Pussy' Trump had for women [Twitter] 6 October*. Available

at: <https://twitter.com/nowthisnews/status/916457058899173376?lang=en> (Accessed: 15 November 2019)

Nicholson, B. (2013) 'The Digital Turn: Exploring the methodological possibilities of digital newspaper archives', *Media History*, 19(1), pp. 59-73.

'Nilo Jerez v. Republic of Cuba, et al.' (2014) United States Court of Appeals, case No. 13-7141. United States Court of Appeals for the District of Columbia Circuit [Online]. Available at: [https://www.cadc.uscourts.gov/internet/opinions.nsf/BEA6FB63E6121EE185257DBE00544C28/\\$file/13-7141-1529572.pdf](https://www.cadc.uscourts.gov/internet/opinions.nsf/BEA6FB63E6121EE185257DBE00544C28/$file/13-7141-1529572.pdf) (Accessed: 28 September 2018).

Nimmo, B. and Barojan, D. (2017) *Fakes, Bots, and Blockings in Armenia. A snapshot of online manipulation on the eve of a parliamentary vote*. Available at: <https://medium.com/dfrlab/fakes-bots-and-blockings-in-armenia-44a4c87ebc46> (Accessed 19 September 2018).

Nimmo, B., Durakgolu, N., Czuperski, M. and Yap, N. (2017) *Hashtag Campaign: #MacronLeaks. Alt-right attacks Macron in last ditch effort to sway French Election*. Available at: <https://medium.com/dfrlab/hashtag-campaign-macronleaks-4a3fb870c4e8> (Accessed 19 September 19, 2018).

Norges Bank Investment Management (2018) *Holdings as at 31.12.2017*. Available at: <https://www.nbim.no/en/the-fund/holdings/holdings-as-at-31.12.2017/> (Accessed: 20 December 2018).

Norris, C. and Armstrong, G. (1999) *The Maximum Surveillance Society: The Rise Of CCTV*. Oxford: Berg.

Nossiter, A., Sanger, D.E. and Perloth, N. (2017) *Hackers Came, but the French Were Prepared*. Available at: <https://www.nytimes.com/2017/05/09/world/europe/hackers-came-but-the-french-were-prepared.html> (Accessed: 9 July 2018).

Nozaki, Y. (2002) 'Japanese politics and the history textbook controversy, 1982–2001', *International Journal of Educational Research*, 37(6-7), pp. 603-622.

Obama White House (2014) *Remarks by the President on Review of Signals Intelligence*  
Available at: <https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence> (Accessed: 4 May 2017).

Obama White House (2016[a]) *President Obama Holds a Press Conference*. Available at: <https://www.youtube.com/watch?v=PkRLXgwy7g> (Accessed: 12 September 2018).

Obama White House (2016[b]) *Remarks by the President on the Administration's Approach to Counterterrorism*. Available at: <https://obamawhitehouse.archives.gov/the-press-office/2016/12/06/remarks-president-administrations-approach-counterterrorism> (Accessed: 25 May 2019).

Office for Science (UK) (2016) *The Quantum Age: Technological opportunities*. Available at: [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/564946/g-s-16-18-quantum-technologies-report.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/564946/g-s-16-18-quantum-technologies-report.pdf) (Accessed: 10 December 2017).

Office of the Director of National Intelligence (2017[a]) *Statement for the Record Worldwide Threat Assessment of the US Intelligence Community Senate Select Committee on Intelligence*. Available at: <https://www.dni.gov/files/documents/Newsroom/Testimonies/SSCI%20Unclassified%20SFR%20-%20Final.pdf> (Accessed: 2 November 2018).

Office of the Director of National Intelligence (2017[b]) *Assessing Russian Activities and Intentions in Recent US Elections* Available at: [https://www.dni.gov/files/documents/ICA\\_2017\\_01.pdf](https://www.dni.gov/files/documents/ICA_2017_01.pdf) (Accessed: 8 January 2017).

Office of the Historian (n.d.[a]) Khrushchev and the Twentieth Congress of the Communist Party, 1956. Available at: <https://history.state.gov/milestones/1953-1960/khrushchev-20th-congress> (Accessed: 6 November 2019)

Office of the Historian (n.d.[b]) *Note on U.S. Covert Actions*. Available at: <https://history.state.gov/historicaldocuments/frus1964-68v12/actionsstatement> (Accessed: 15 June 2018).

Office of the Historian (n.d.[c]) *U.S. Diplomacy and Yellow Journalism, 1895–1898*. Available at: <https://history.state.gov/milestones/1866-1898/yellow-journalism> (Accessed: 2 January 2016).

Office of the Historian (n.d.[d]) *192. Report by the Special Study Group: Report on the Covert Activities of the Central Intelligence Agency*. Available at: <https://history.state.gov/historicaldocuments/frus1950-55Intel/d192> (Accessed: 29 April 2019).

Office of the Historian (1947) *Memorandum by the Acting Director of the Office of European Affairs (Reber) to the Acting Secretary of State: Present Italian Situation; Implementation of NSC 1/1 "The Position of the United States with Respect to Italy*. Available at: <https://history.state.gov/historicaldocuments/frus1948v03/d441> (Accessed: 11 July 2018).

Office of the Historian (1948[a]) *Report by the National Security Council: The Position of the United States With Respect to Italy*. Available at: <https://history.state.gov/historicaldocuments/frus1948v03/d469> (Accessed: 11 July 2018).

Office of the Historian (1948[b]) *292. National Security Council Directive on Office of Special Projects: NSC 10/2*. Available at: <https://history.state.gov/historicaldocuments/frus1945-50Intel/d292> (Accessed: 25 September 2018).



Office of the Historian (1954) *Memorandum by the Director of Central Intelligence (Dulles) to the President: The attached summary of the situation in Guatemala as of today is submitted at the suggestion of Mr. Allen Dulles.* Available at: <https://history.state.gov/historicaldocuments/frus1952-54v04/d476> (Accessed: 25 September 2018).

Office of the Historian (1955) 259. *National Security Council Intelligence Directive No. 17: "Electronic Intelligence" (ELINT).* Available at: <https://history.state.gov/historicaldocuments/frus1950-55Intel/d259> (Accessed: 22 December 2018).

Office of the Historian (1965) 110. *Memorandum Prepared for the 303 Committee: Progress Report on [less than 1 line of source text not declassified] Covert Action in Indonesia.* Available at: <https://history.state.gov/historicaldocuments/frus1964-68v26/d110> (Accessed: 24 May 2019).

Office of the Historian (1975) 287. *Memorandum Prepared in the Central Intelligence Agency: CIA's Role in the Overthrow of Arbenz: CIA's Role in the Overthrow of Arbenz.* Available at: <https://history.state.gov/historicaldocuments/frus1952-54Guat/d287> (Accessed: 26 October 2018).

Office of the Legislative Counsel U.S. House of Representatives (2013) *American Service Members' Protection Act 2002.* Available at: <https://legcounsel.house.gov/Comps/aspa02.pdf> (Accessed: 3 November 2019)

Office of the United Nations High Commissioner for Human Rights (2018[a]) *The Right to Privacy in the Digital Age.* Available at: <https://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx> (Accessed: 10 July 2018).

Office of the United Nations High Commissioner for Human Rights (2018[b]) *Too much surveillance: Respect civil liberties and stop playing 'fear card', says UN expert.*

Available at:

<https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=21321>

(Accessed: 10 July 2018).

Office of the United Nations High Commissioner for Human Rights, (2019[a]) *International Covenant on Civil and Political Rights*. Available at:

<https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx> (Accessed 4 November 2019).

Office of the United Nations High Commissioner for Human Rights, (2019[b]) Sudan: UN experts denounce Internet shutdown, call for immediate restoration. Available at:

<https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24803&LangID=E> (Accessed: 11 December 2019)

O'Hara, K. and Shadbolt, N. (2008) *The Spy In The Coffee Machine*. Oxford: Oneworld.

Omand, D. (2009) *The National Security Strategy: Implications for the UK intelligence community*. Available at:

[https://warwick.ac.uk/fac/soc/pais/people/aldrich/vigilant/national\\_security\\_strategy1.pdf](https://warwick.ac.uk/fac/soc/pais/people/aldrich/vigilant/national_security_strategy1.pdf) (Accessed: 4 April 2009).

Omand, D. and Phythian, m. (2013) 'Ethics and Intelligence: 'A Debate'', *International Journal of Intelligence and CounterIntelligence*, 26(1), pp. 38-63.

Osborne, H. and Cutler, S. (2019) *Chinese border guards put secret surveillance app on tourists' phones*. Available at: <https://www.theguardian.com/world/2019/jul/02/chinese-border-guards-surveillance-app-tourists-phones> (Accessed: 25 October 2019)

Osorio, C., Tandeciarz, S. and Weech, J. (2019) *Inside Argentina's Killing Machine: U.S. Intelligence Documents Record Gruesome Human Rights Crimes of 1976-1983*.

Available at: <https://nsarchive.gwu.edu/briefing-book/southern-cone/2019-05-30/inside-argentinas-killing-machine-us-intelligence-documents-record-gruesome-human-rights-crimes-1976> (Accessed: 2 January 2020)

Oxford Dictionary (2018) *Cooperation*. Available at:

<https://en.oxforddictionaries.com/definition/cooperation> (Accessed: 16 December 2018).

PBS (n.d.) "Diseases and Peculiarities of the Negro Race". Available at:

<https://www.pbs.org/wgbh/aia/part4/4h3106t.html> (Accessed: 5 November 2019).

Palantir (2019) *PALANTIR GOTHAM: Integrate, manage, secure, and analyze all of your enterprise data*. Available: <https://www.palantir.com/palantir-gotham/> Accessed (14 November 2019)

Paolucci, P. (2009) 'Public discourse in an age of deception: forging the Iraq War', *Critical Sociology*, 35(6), pp.863-886.

Parker, J. (2000) *Total Surveillance Investigating. The Big Brother World of E-Spies, Eavesdroppers and CCTV*. London: Piatkus.

Parliament (UK) (n.d.) *The contents of Magna Carta*. Available at:

<https://www.parliament.uk/about/living-heritage/evolutionofparliament/originsofparliament/birthofparliament/overview/magnacarta/magnacartaclauses/> (Accessed: 30 November 2019)

Parliament. House of Commons (2016[a]) *Intelligence and Security Committee of Parliament: Report on the draft Investigatory Powers Bill* (HC 795). London: The Stationery Office.

Parliament. House of Commons (2016[b]) *The report of the Iraq Inquiry: report of a committee of Privy Counsellors, volume IV*. (HC 265-IV). London: The Stationery Office.

Parliament. House of Commons (2017) *Intelligence and Security Committee of Parliament Annual Report 2016 – 2017* (HC 655). London: The Stationery Office.

- Parliament. House of Commons (2019) *Disinformation and 'fake news': Final Report*. (HC 1791). London. Available at:  
<https://publications.parliament.uk/pa/cm201719/cmselect/cmcomeds/1791/1791.pdf>  
 (Accessed: 2 January 2020)
- Patel, T.G. (2012) 'Surveillance, suspicion and stigma: Brown bodies in a terror-panic climate', *Surveillance & Society*, 10(3/4), pp. 215 – 232.
- Paul, C. (2010) *Psychological Operations by Another Name Are Sweeter*. Available at:  
<https://www.rand.org/blog/2010/07/psychological-operations-by-another-name-are-sweeter.html> (Accessed: 27 February 2018).
- 'Payton v. New York' (1980) The Court Of Appeals of New York, Case No.78-5420. Available at: <http://cdn.loc.gov/service/ll/usrep/usrep445/usrep445573/usrep445573.pdf>  
 (Accessed: 3 January 2020).
- Pedlow, G.W. and Welzenbach, D.E. (1992) *The Central Intelligence Agency and Overhead Reconnaissance: The U-2 and OXCART Programs, 1954-1974*. Available at:  
[https://www.cia.gov/library/readingroom/docs/DOC\\_0000192682.pdf](https://www.cia.gov/library/readingroom/docs/DOC_0000192682.pdf) (Accessed: 1 November 2019)
- Pennington, D.C., Gillen, K. and Hill, P. (1999) *Social Psychology*. London: Arnold.
- Perez, L. A. (2008) *Cuba in the American Imagination: Metaphor and the Imperial Ethos*. North Carolina: The University of North Carolina Press.
- Pevehouse, J.C.W. and Goldstein, J.S. (2017) *International Relations. 11<sup>th</sup> edn*. Boston: Pearson.
- Pew Research Center, 2017, Stark Partisan Divisions Over Russia Probe, Including Its Importance to the Nation. Available at: <https://www.people-press.org/2017/12/07/stark-partisan-divisions-over-russia-probe-including-its-importance-to-the-nation/> (Accessed: 3 June 2019).

- Pfau, M., Haigh, M.M., Logsdon, L., Perrine, C., Baldwin, J.P., Breitenfeldt, R.E., Cesar, J., Dearden, D., Kuntz, G., Montalvo, E., Roberts, D & Romero, R. (2005) 'Embedded Reporting During the Invasion and Occupation of Iraq: How the Embedding of Journalists Affects Television News Reports', *Journal of Broadcasting & Electronic Media*, 49(4), pp. 468-487.
- Pickering, M. (2001) *Stereotyping: The politics of Representation*. Basingstoke: Palgrave
- Pihama, L., Reynolds, P., Smith, C., Reid, J., Smith, L.T. and Nana, R.T. (2014) 'Positioning historical trauma theory within Aotearoa New Zealand', *AlterNative: An International Journal of Indigenous Peoples*, 10(3), pp.248-262.
- Pompeo, M. (2017) *Director Pompeo Delivers Remarks at CSIS*. Available at: <https://www.cia.gov/news-information/speeches-testimony/2017-speeches-testimony/pompeo-delivers-remarks-at-csis.html> (Accessed: 8 December 2019)
- Porch, D (1997) *The French Secret Services: From the Dreyfus Affair to the Gulf War*. Oxford: Oxford University Press.
- Porup, J.M. (2015) *How Mexican Twitter Bots Shut Down Dissent*. Available at: <http://motherboard.vice.com/read/how-mexican-twitter-bots-shut-down-dissent> (Accessed: 5 July 2016).
- PowerfulJRE (2019) *Joe Rogan Experience #1255 - Alex Jones Returns!* Available at: <https://www.youtube.com/watch?v=-5yh2HcIlkU&t=7879s> (Accessed: 1 January 2020)
- Prime Minister's Office., Department for International Development., Foreign and Commonwealth Office., Home Office., Ministry of Defence., and May, T. (2018) *UK to step up French operations in Africa as PM and President Macron meet for UK-France Summit*. Available at: <https://www.gov.uk/government/news/uk-to-step-up-french-operations-in-africa-as-pm-and-president-macron-meet-for-uk-france-summit> (Accessed: 12 February 2019).

- Proctor, K. (2019) *Brexit: Boris Johnson apologises to Tory members for deadline extension*. Available at: <https://www.theguardian.com/politics/2019/nov/03/boris-johnson-apologises-tory-members-not-leaving-eu-october> (Accessed: 1 January 2020)
- ‘Prosecutor v. Dusko Tadic aka "Dule"' (1997) *International Criminal Tribunal for the former Yugoslavia (ICTY), Case No. IT-94-I-T* [Online] Available at: <https://www.icty.org/x/cases/tadic/tjug/en/tad-tsj70507JT2-e.pdf> (Accessed: 10 December 2019).
- Public Relations and Communications Association (2019) *Bell Pottinger case study*. Available at: <https://www.prca.org.uk/campaigns/ethics/bell-pottinger-case-study> (Accessed: 20 November 2019)
- Quinlan, M. (2007) ‘Just intelligence: Prolegomena to an ethical theory’, *Intelligence and National Security*, 22(1), pp. 1-13.
- Ranelagh, J. (1988) *The Agency The Rise & Decline Of The CIA*. London: Sceptre
- Ratkiewicz, J., Conover, M., Meiss, M.R., Gonçalves, B., Flammini, A. and Menczer, F. (2011) ‘Detecting and tracking political abuse in social media’, *Proceedings of the Fifth International AAAI Conference on Weblogs and Social Media*, Barcelona, Spain, 17 – 21 July. The AAAI Press. Available at: <https://www.aaai.org/ocs/index.php/ICWSM/ICWSM11/paper/viewFile/2850/3274> (Accessed: 1 November 2018).
- Rawlinson, K. and Dodd, V. (2019) *Shamima Begum: Isis Briton faces move to revoke citizenship*. Available at: <https://www.theguardian.com/world/2019/feb/19/isis-briton-shamima-begum-to-have-uk-citizenship-revoked> (Accessed: 28 February 2019).
- Rawnsley, A. (2019) *There’s no more deceptive slogan of this campaign than ‘get Brexit done’*. Available at: <https://www.theguardian.com/commentisfree/2019/nov/24/there-is-no-more-deceptive-slogan-of-this-campaign-than-get-brexit-done> (Accessed: 6 December 2019)

Regina v. Looseley (2001) House of Lords. Available at:

<https://publications.parliament.uk/pa/ld200102/ldjudgmt/jd011025/loose-1.htm>

(Accessed: 18 December 2019)

Reid, K., Flowers, P. and Larkin, M. (2005) 'Exploring lived experience', *The Psychologist*, 18(1), pp.20-23.

Reinold, T. (2013) *Soverignty and the Responsibility to Protect: The power of norms the norms of the powerful*. Abingdon: Routledge

Reitman, R. (2017) *Who Has Your Back? Government Data Requests 2017*. Available at:

<https://www.eff.org/who-has-your-back-2017> (Accessed: 27 April 2018).

Rentoul, R. R. (1906) *Race Culture, Or, Race Suicide? A Plea for the Unborn*. London, The Walter Scott publishing.

Reuters (2016) *United States Senate*. Available at:

<http://fingfx.thomsonreuters.com/gfx/rngs/USA-ELECTION-DOCUMENTS/010030ET0X4/letter.jpg> (Accessed: 28 June 2018).

Richards, J. (2012) 'Intelligence dilemma? Contemporary counter-terrorism in a liberal democracy', *Intelligence and national security*, 27(5), pp. 761-780.

Roll-Hansen, N. (1989) 'Geneticists and the eugenics movement in Scandinavia', *The British Journal for the History of Science*, 22(3), pp.335-346.

Ronn, K.V. (2016) 'Intelligence Ethics: A Critical Review and Future: Perspectives', *International Journal of Intelligence and CounterIntelligence*, 29(4), pp. 760-784.

Rose, M. and Dyomkin, D. (2017) *After talks, France's Macron hits out at Russian media, Putin denies hacking*. Available at: <https://www.reuters.com/article/us-france->

[russia/after-talks-frances-macron-hits-out-at-russian-media-putin-denies-hacking-idUSKBN18P030](https://www.reuters.com/article/uk-france-nato-braindead/frances-macron-im-not-sorry-i-called-nato-brain-dead-idUSKBN18P030) (Accessed: 12 July 2018).

Rose, M. (2019) France's Macron: I'm not sorry I called NATO brain dead. Available at: <https://uk.reuters.com/article/uk-france-nato-braindead/frances-macron-im-not-sorry-i-called-nato-brain-dead-idUKKBN1Y21FY> (Accessed: 20 December 2019)

Rosenau, W. and Long, A. (2009) *The Phoenix Program and Contemporary Counterinsurgency*. Available at: [https://www.rand.org/content/dam/rand/pubs/occasional\\_papers/2009/RAND\\_OP258.pdf](https://www.rand.org/content/dam/rand/pubs/occasional_papers/2009/RAND_OP258.pdf) (Accessed: 24 April 2018).

Ross, J. I. (2000) *Varirties of State Crime and its Control* (ed). New York: Criminal Justice Press.

Roucek, J.S. (1956) *Social control*. 2<sup>nd</sup> edn. Connecticut: Greenwood Press.

'Roy Cockrum, ET AL. v Donald J. Trump for President' (2018) United States District Court for the Eastern District of Virginia Richmond Division, Case No. 3:18-cv-484-HEH [Online]. Available at: <https://www.justsecurity.org/wp-content/uploads/2018/10/Trump-Campaign-Cockburn-Brief-10-08-2018-1.pdf> (Accessed: 8 December 2019)

RT (2014[a]) *Exactly how the US trained and armed ISIS*. Available at: <https://www.youtube.com/watch?v=XnU6P2T5Yr4> (Accessed: 10 July 2018).

RT (2014[b]) *'ISIS is CIA false flag op, pretext for war inside Syria & Iraq'*. Available at: <https://www.youtube.com/watch?v=j5OYeBQdrFE> (Accessed: 10 July 2018).

RT (2017) *US 'created the monster' of Taliban, ISIS – fmr Pentagon official*. Available at: <https://www.youtube.com/watch?v=Vi0CZ1VYVP0> (Accessed: 10 July 2018).



- RT (2018[a]) #ICYMI: *The Skripals were poisoned and the guinea pigs died. What a Novi-cock up!*. Available at: <https://www.rt.com/shows/icymi-with-polly-boiko/424043-skripal-saga-novichok-nerve-agent/> (Accessed: 22 November 2018)
- RT (2018[b]) 15 years after Iraq War, same old MPs jump on chemical weapons claims in Skripal poisoning. Available at: <https://www.rt.com/uk/421849-mps-iraq-war-russia/> (Accessed: 22 November 2019)
- RT (2018[c]) *Lavrov: Intel services of 'a state' that promotes Russophobia behind 'staged' Douma chemical attack*. Available at: <https://www.rt.com/news/424007-lavrov-syria-staged-attack/> (Accessed: 12 June 2018).
- Rudnik, L., Miller, D. B. and Levy, L. (2015) *Towards Cyber Stability. A User-Centred Tool for Policymakers*. Available at: <http://www.unidir.org/files/publications/pdfs/cyber-index-2014-en-625.pdf> (Accessed: 13 February 2018).
- Ruiz, M. (2019) *So, President Trump, Should Your Wife "Go Back" to Her Country, Too?*. Available at: <https://www.vogue.com/article/trump-congresswomen-racist-tweets-reaction> (Accessed: 1 January 2020)
- Rumelili, B. and Çelik, A. B. (2017) 'Ontological insecurity in asymmetric conflicts: Reflections on agonistic peace in Turkey's Kurdish issue', *Security Dialogue*, 48(4), pp. 279-296.
- Rumold, M. (2016) *Playpen: The Story of the FBI's Unprecedented and Illegal Hacking Operation*. Available at: <https://www.eff.org/deeplinks/2016/09/playpen-story-fbis-unprecedented-and-illegal-hacking-operation> (Accessed: 10 December 2019)
- Rupert, M. (2010) 'Marxism', In Dunne, T., Kurji, M. and Smith, S. 3rd edn, *International Relations Theories: Discipline and Diversity*. Oxford: Oxford University Press, pp.151 – 170.

- Russia Direct Investment Fund (2018) *Russia Direct Investment Fund*. Available at: [https://rdif.ru/Eng\\_Partnership/](https://rdif.ru/Eng_Partnership/) (Accessed: 20 December 2018).
- Ryan, M. and Switzer, L. (2009) 'Propaganda and the subversion of objectivity: media coverage of the war on terrorism in Iraq, *Critical Studies on Terrorism*', 2(1), pp. 45-64.
- Rydstrom, H. (2015) 'Politics of colonial violence: Gendered atrocities in French occupied Vietnam', *European Journal of Women's Studies*, 22(2), pp.191-207.
- Saddique, H. and French, M. (2010) *Bloody Sunday inquiry: key findings*. Available at: <https://www.theguardian.com/uk/2010/jun/15/bloody-sunday-inquiry-key-findings> (Accessed: 30 November 2019)
- Salehyan, I. (2018) *Should Robert Bowers, the Pittsburgh synagogue shooting suspect be called a terrorist?* Available at: <https://www.google.com/amp/s/www.washingtonpost.com/amphtml/news/monkey-cage/wp/2018/11/01/should-robert-bowers-the-pittsburgh-synagogue-shooting-suspect-be-called-a-terrorist/> (Accessed: 1 March 2019).
- San-Akca, B. (2014) 'Democracy and Vulnerability: An Exploitation Theory of Democracies by Terrorists', *Journal of Conflict Resolution*, 58(7), pp. 1285-1310.
- Sarantakos, S. (2013) *Social Research*. 4<sup>th</sup> edn. London: Palgrave Macmillan.
- Sartre, J-P. (2003) *Being and Nothingness*. Translated by Warnock, M. Rev. edn. London: Routledge Classics.
- Save the Children (n.d.) *Africa. Helping children change the world*. Available at: <https://www.savethechildren.org.uk/where-we-work/africa> (Accessed: 11 November 2018).

- Schneier on Security (2018) *Two NSA Algorithms Rejected by the ISO*. Available at: [https://www.schneier.com/blog/archives/2018/04/two\\_nsa\\_algorit.html](https://www.schneier.com/blog/archives/2018/04/two_nsa_algorit.html) (Accessed: 29 April 2019).
- Schrock, A.R. (2016) 'Civic hacking as data activism and advocacy: A history from publicity to open government data', *New Media & Society*, 18(4), pp.581-599.
- Schroepfer, M. (2018) *An Update on Our Plans to Restrict Data Access on Facebook*. Available at: <https://about.fb.com/news/2018/04/restricting-data-access/> (Accessed: 14 November 2019)
- Schuch, J. (2017) 'Negotiating the limits of upbringing, education, and racial hygiene in Nazi Germany as exemplified in the study and treatment of Sinti and Roma', *Race Ethnicity and Education*, 20(5), pp.609-623.
- Schultz, A. (1970) 'Alfred Schutz on Phenomenology and Social Relations: Selected Writings', In Wagenr, H. (ed.) *On Phenomenology and Social Relations: Selected Writings*. Chicago: University of Chicago Press.
- Schulze, M. (2015) 'Patterns of surveillance legitimization. The German discourse on the NSA scandal', *Surveillance & Society*, 13(2), pp.197-217.
- Sciutto, J. (2017) *How one typo helped let Russian hackers in*. Available at: <https://edition.cnn.com/2017/06/27/politics/russia-dnc-hacking-csr/index.html> (Accessed: 24 May 2018).
- Scott-Railton, J., Marquis-Boire, M., Guarnieri, C., Marschalek, M. (2015) *Packrat Seven Years of a South American Threat Actor*. Available at: <https://citizenlab.ca/2015/12/packrat-report/> (Accessed: 2 June 2019).
- Sessions, J. (2017) *Attorney General Jeff Sessions Delivers Remarks at Briefing on Leaks of Classified Materials Threatening National Security*. Available at:

<https://www.justice.gov/opa/pr/attorney-general-jeff-sessions-delivers-remarks-briefing-leaks-classified-materials> (Accessed: 30 November 2018).

Shane, S. (2006) *An Exotic Tool for Espionage: Moral Compass*. Available at: <https://www.nytimes.com/2006/01/28/politics/an-exotic-tool-for-espionage-moral-compass.html> (Accessed: 14 April 2019).

Shaw, T. (1999) 'The Information Research Department of the British Foreign Office and the Korean War, 1950–53', *Journal of Contemporary History*, 34(2), pp.263-281.

Shelton, A.M. (2011) 'Framing the oxymoron: A new paradigm for intelligence ethics', *Intelligence and National Security*, 26(1), pp. 23-45.

Shepardson, D. (2019) *Facebook, Google accused of anti-conservative bias at U.S. Senate hearing*. Available at: <https://www.reuters.com/article/us-usa-congress-socialmedia/facebook-google-accused-of-anti-conservative-bias-at-u-s-senate-hearing-idUSKCN1RM2SJ> (Accessed: 8 December 2019)

Shiffman, J. Cooke, K. and Hosenball, M. (2013) *Insight: FBI relies on secret U.S. surveillance law, records show*. Available at: <https://www.reuters.com/article/us-usa-security-fisa-insight/insight-fbi-relies-on-secret-u-s-surveillance-law-records-show-idUSBRE95H03220130618> (Accessed: 3 January 2019)

Shiraz, Z. (2013) 'Drugs and Dirty Wars: intelligence cooperation in the global South', *Third World Quarterly*, 34(10), pp. 1749-1766.

Shirbon, E. (2019) *Twitter says Conservatives misled public, minister says voters 'don't give a toss'*. Available at: <https://uk.reuters.com/article/uk-britain-election-twitter/twitter-says-conservatives-misled-public-minister-says-voters-dont-give-a-toss-idUKKBN1XU0RF> (Accessed: 11 December 2019)

- Simon, S.W. (1995) 'Realism and neoliberalism: international relations theory and Southeast Asian security', *The Pacific Review*, 8(1), pp. 5-24.
- Skelton, G. (1985) *Reagan Cites 'Terrorist Nations' for 'War Acts' : Points to Iran, Libya, North Korea, Nicaragua and Cuba, Says U.S. 'Has Right to Defend Itself'*. Available at: <https://www.latimes.com/archives/la-xpm-1985-07-09-mn-8079-story.html> (Accessed: 26 December 2019)
- Smith, L. (1980) 'Covert British Propaganda: The information research department: 1947-771', *Millennium*, 9(1), pp.67-83.
- Smith, N.D. (1983) 'Aristotle's Theory of Natural Slavery', *Phoenix*, 37(2), pp.109-122.
- Smith, B.F. (1988) 'Sharing Ultra in World War II', *International Journal of Intelligence and Counter Intelligence*, 2(1), pp. 59-72.
- Smith, J. A. and Osborn, M. (2015) 'Interpretative Phenomenological Analysis' in J.A. Smith *Qualitative psychology: A Practical Guide to Research Methods*. 3<sup>rd</sup> edn. London: Sage, pp. 25 – 52.
- Smith, B. (2017[a]) *The need for urgent collective action to keep people safe online: Lessons from last week's cyberattack*. Available at: <https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/> (Accessed: 20 December 2018).
- Smith, B. (2017[b]) *The need for a Digital Geneva Convention*. Available at: <https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/> (Accessed: 12 January 2018).
- Smith, B. (2017[c]) *We need to modernize international agreements to create a safer digital world*. Available at: <https://blogs.microsoft.com/on-the-issues/2017/11/10/need->

modernize-international-agreements-create-safer-digital-world/ (Accessed: 13 February).

Smith, A. (2019) Trump says congresswomen of color should 'go back' and fix the places they 'originally came from'. Available at: <https://www.nbcnews.com/politics/donald-trump/trump-says-progressive-congresswomen-should-go-back-where-they-came-n1029676> (Accessed: 1 January 2020)

South China Morning Post (2019) *Carrie Lam addresses extradition law controversy*. Available at: <https://www.youtube.com/watch?v=HhgR6dCjKvg> (Accessed: Accessed: 2 January 2020)

Spinelli, E. (2005) *The interpreted world an introduction to phenomenological psychology*. London: SAGE

Spruds, A., Rožukalne, A., Sedlenieks, K., Daugulis, M., Potjomkina, D., Tölgyesi, B., Bruge, I. (2016) *Internet Trolling As a Tool of Hybrid Warfare: The Case of Latvia*. Available at: <https://www.stratcomcoe.org/internet-trolling-hybrid-warfare-tool-case-latvia-0> (Accessed: 21 October 2018).

Srivastava, J. and Sharma, A. (2017) 'International Relations Theory and World Order: Binaries, Silences and Alternatives', *South Asian Survey*, 21(1-2), pp. 20-34.

Stack, L. (2016) *He Calls Hillary Clinton a 'Demon' Who Is Alex Jones?* Available at: <https://www.nytimes.com/2016/10/14/us/politics/alex-jones.html> (Accessed: 31 December 2018).

Stanford University (n.d.) Federal Bureau of Investigation (FBI). Available at: <https://kinginstitute.stanford.edu/encyclopedia/federal-bureau-investigation-fbi> (Accessed: 6 November 2019)

- Steele, B. J. (2017) 'Organizational processes and ontological (in) security: Torture, the CIA and the United States', *Cooperation and Conflict*, 52(1), pp. 69-89.
- Stein, A. A. (2010) 'Neoliberal Institutionalism' in Reus-Smit, C. and Snidal, D. (ed.) *The Oxford Handbook of International Relations*. Oxford: Oxford University Press, pp. 201-221.
- Steinhauser, P and Helton, J. (2013) *CNN poll: Public against Syria strike resolution*. Available at: <https://edition.cnn.com/2013/09/09/politics/syria-poll-main/index.html> (Accessed: 19 November 2019)
- Stephens, B. (2019) *World War II and the Ingredients of Slaughter: The spirit of certitude that dominated the politics of the 1930s is not so distant from us today*. Available at: <https://www.nytimes.com/2019/08/30/opinion/world-war-ii-anniversary.html> (Accessed: 10 November 2019)
- Stern, G. (2000) *The Structure of International Society. An Introduction to the Study of International Relations*. 2<sup>nd</sup> edn. London: Pinter.
- Stern, M. (2006) 'We' the subject: The power and failure of (in) security', *Security Dialogue*, 37(2), pp. 187-205.
- Stevens, M. (2019) *Elizabeth Warren on Breaking Up Big Tech*. Available at: <https://www.nytimes.com/2019/06/26/us/politics/elizabeth-warren-break-up-amazon-facebook.html> (Accessed: 13 Decemebr 2019)
- Stone, J. (2019) *UK government doesn't understand how EU works, says its former ambassador to Brussels Ivan Rogers*. Available at: <https://www.independent.co.uk/news/uk/politics/uk-understand-eu-works-brexit-ivan-rogers-a8806931.html> (Accessed: 1 January 2020)

StopFake (2017) *Russia's New 'Useful Idiots'?* Available at:

[https://www.stopfake.org/en/tag/useful-idiots/?\\_cf\\_chl\\_jschl\\_tk\\_\\_=47d89ba56c05548b4de93e7ee2caeb2405bdae5b-1576005093-0-AbgK-PtyFocNQ1RpiHKrm4\\_3vocKNRVAEuYwdlYQ6uYHyJ0KV3j-kJDYUeL48tBqwOr6zKrD6b-0Tw8AL7bWbLMmpP784tbC\\_vUfYgccJTJRZuO2jFOgKNp6EYyasIz1NV9c3KLq6ZhvDP0ZA6A-BiGIF7cEsOiobeMkXTcf47kywf\\_tKzOpqA6nCmyOIXuWd39K4WysBd5w9gyvvkNrzcd73wOKI0fZFc9lFtd8EB3\\_Mv0VSZFW2Epm3Xr\\_4wyU5zpupjCjt\\_3hwhYKXLgCyzRTrmdMqJq1dnUDloxqkyi-](https://www.stopfake.org/en/tag/useful-idiots/?_cf_chl_jschl_tk__=47d89ba56c05548b4de93e7ee2caeb2405bdae5b-1576005093-0-AbgK-PtyFocNQ1RpiHKrm4_3vocKNRVAEuYwdlYQ6uYHyJ0KV3j-kJDYUeL48tBqwOr6zKrD6b-0Tw8AL7bWbLMmpP784tbC_vUfYgccJTJRZuO2jFOgKNp6EYyasIz1NV9c3KLq6ZhvDP0ZA6A-BiGIF7cEsOiobeMkXTcf47kywf_tKzOpqA6nCmyOIXuWd39K4WysBd5w9gyvvkNrzcd73wOKI0fZFc9lFtd8EB3_Mv0VSZFW2Epm3Xr_4wyU5zpupjCjt_3hwhYKXLgCyzRTrmdMqJq1dnUDloxqkyi-) (Accessed: 10 December 2019)

Stoycheff, E. (2016) 'Under surveillance: Examining Facebook's spiral of silence effects in the wake of NSA internet monitoring', *Journalism & Mass Communication Quarterly*, 93(2), pp.296-311.

Solberg, J. (2012) 'Googling the Archive: Digital Tools and the Practice of History', *Advances in the History of Rhetoric*, 15(1), pp. 53-76.

Solsvik, T. and Fouche, G. (2017) *Norway wealth fund hits record \$1 trillion ahead of revamp*. Available at: <https://www.reuters.com/article/us-norway-swf/norway-wealth-fund-hits-record-1-trillion-ahead-of-revamp-idUSKCN1BN17G> (Accessed: 1 January 2019).

Subotić, J. (2016) 'Narrative, ontological security, and foreign policy change', *Foreign Policy Analysis*, 12(4), pp. 610-627.

Sunderland, R (1964) *Antiguerrilla Intelligence in Malaya, 1948 – 1960*. Available at: [https://www.rand.org/content/dam/rand/pubs/research\\_memoranda/2005/RM4172.pdf](https://www.rand.org/content/dam/rand/pubs/research_memoranda/2005/RM4172.pdf) (Accessed: 25 April 2020)

Sullivan, J. (2014) 'China's Weibo: Is faster different?', *New Media & Society*, 16(1), pp. 24-37.



- Suwajanakorn, S., Seitz, S.M. and Kemelmacher-Shlizerman, I. (2017) 'Synthesizing Obama: Learning Lip Sync from Audio', *ACM Transactions on Graphics*, 36(4), pp.1-13.
- Taliaferro, J.W. (2001) 'Security seeking under anarchy: Defensive realism revisited', *International security*, 25(3), pp. 128-161.
- Tawil, D.D. (2000) '" Ready? Induce. Sting!": Arguing for the Government's Burden of Proving Readiness in Entrapment Cases', *Michigan Law Review*, 98(7), pp.2371-2394.
- Taylor, P.M. (2002) 'Strategic Communications or Democratic Propaganda?', *Journalism Studies*, 3(3), pp. 437-441.
- Teaching American History, (2019[a]) *Message to Grassroots*. Available at: <https://teachingamericanhistory.org/library/document/message-to-grassroots/> (Accessed: 3 November 2019)
- Teaching American History, (2019[b]) *The Ballot or the Bullet*. Available at: <https://teachingamericanhistory.org/library/document/the-ballot-or-the-bullet/> (Accessed: 3 November 2019).
- The American Presidency Project (n.d.) *Address Before a Joint Session of Congress on the State of the Union*. Available at: <https://www.presidency.ucsb.edu/documents/address-before-joint-session-congress-the-state-the-union-0#axzz1xnQLFdLi> (Accessed: 16 November 2019)
- The Breakfast Club (2019) *Maury Talks New Board Game, 2020 Candidates, Relationships + More*. Available at: <https://www.youtube.com/watch?v=6HFzH1HT2LM> (Accessed: 20 November 2019)
- The British Library (n.d.) *Civilians*. Available at: <https://www.bl.uk/world-war-one/themes/civilians> (Accessed: 26 October 2018).

- The British Library (2014) *Atrocity propaganda in World War One*. Available at: [https://www.youtube.com/watch?time\\_continue=20&v=YeGveZWF500](https://www.youtube.com/watch?time_continue=20&v=YeGveZWF500) (Accessed 24 September 2018).
- The Bureau of Investigative Journalism (2017) *A firsthand account of Bell Pottinger's top secret work in Iraq*. Available at: <https://vimeo.com/183694713> (Accessed: 20 December 2017).
- The Center of Law and Security (2011) *Terrorist Trial Report Card: September 11, 2001 – September 11, 2011*. Available at: <https://www.lawandsecurity.org/wp-content/uploads/2011/09/TTRC-Ten-Year-Issue.pdf> (Accessed: 10 January 2017).
- The Computational Propaganda Research Project (2016) *The Computational Propaganda Research Project. Algorithms, Automation and Digital Politics*. Available at: <http://comprop.oii.ox.ac.uk/page/5/> (Accessed: 7 July 2018).
- The Courage Foundation (n.d.) *Computer Network Exploitation*. Available at: <https://edwardsnowden.com/2018/06/01/computer-network-exploitation/> (Accessed: 27 December 2018).
- The Courage Foundation, (2014[a]) *Shotgiant*. Available at: <https://edwardsnowden.com/2014/03/22/shotgiant/> (Accessed: 11 December 2019)
- The Courage Foundation (2014[b]) *TURBINE*. Available at: <https://edwardsnowden.com/2014/03/12/turbine/> (Accessed: 20 November 2017).
- The Economist (2010) *In defence of WikiLeaks*. Available at: <https://www.economist.com/democracy-in-america/2010/11/29/in-defence-of-wikileaks> (Accessed: 06 November 2010).

The Electoral Commission (2019) *Media statement: Vote Leave*. Available at:

<https://www.electoralcommission.org.uk/media-statement-vote-leave> (Accessed: 14 November 2019)

The Guardian (2014) *'I can't breathe': Eric Garner put in chokehold by NYPD officer – video*.

Available at: <https://www.theguardian.com/us-news/video/2014/dec/04/i-cant-breathe-eric-garner-chokehold-death-video> (Accessed: 1 March 2019).

The Guardian (2016) *Let's talk about immigration: EU Referendum – Brexit 2016*. Available at:

<https://www.youtube.com/watch?v=X-JvzFb3jEM> (Accessed: 7 December 2019)

The Guardian (2018) *What is the Cambridge Analytica scandal?*. Available at:

[https://www.youtube.com/watch?time\\_continue=128&v=Q91nvbJSmS4&feature=emb\\_title](https://www.youtube.com/watch?time_continue=128&v=Q91nvbJSmS4&feature=emb_title) (Accessed: 2 January 2020)

The Intercept (2014) *The Art of Deception: Training for a New Generation of Online Covert*

*Operations*. Available at: <https://theintercept.com/document/2014/02/24/art-deception-training-new-generation-online-covert-operations/> (Accessed: 2 November 2019)

The Intercept (2015[a]) *Behavioural Science Support for JTRIG's (Joint Threat Research and Intelligence Group's) Effects and Online HUMINT Operations*. Available at:

<https://theintercept.com/document/2015/06/22/behavioural-science-support-jtrig/> (Accessed: 27 September 2018).

The Intercept (2016) *The UN Security Council: (SIGINT) History Repeats Itself!* Available at:

<https://theintercept.com/snowden-sidtoday/3008423-the-un-security-council-sigint-history-repeats/> (Accessed: 17 May 2020)

The Intercept (2015[b]) *Blazing Saddles Tools*. Available at:

<https://theintercept.com/document/2015/09/25/blazing-saddles-tools/> (Accessed: 17 December 2018).

The Intercept (2015[c]) *Cloud Developers Exchange July 2011*. Available at:

<https://theintercept.com/document/2015/09/25/cloud-developers-exchange-july-2011/>

(Accessed: 17 December 2018).

The Intercept (2015[d]) *The Great SIM Heist How Spies Stole the Keys to the Encryption*

*Castle*. Available at: <https://theintercept.com/2015/02/19/great-sim-heist/> (Accessed: 27

April 2018).

The Intercept (2015[e]) *PCS Harvesting at Scale*. Available at:

<https://theintercept.com/document/2015/02/19/pcs-harvesting-scale/> (Accessed: 27

April 2018).

The Intercept (2015[f]) *DAPINO GAMMA Gemalto Yuaawaa Wiki*. Available at:

<https://theintercept.com/document/2015/02/19/dapino-gamma-gemalto-yuaawaa-wiki/>

(Accessed: 27 April 2018).

The National Archives (UK) (n.d.[a]) *Internees*. Available at:

<http://www.nationalarchives.gov.uk/help-with-your-research/research-guides/internees/>

(Accessed: 25 April 2018).

The National Archives (UK) (n.d.[b]) *Alleged German 'war crimes'*. Available at:

<http://www.nationalarchives.gov.uk/pathways/firstworldwar/spotlights/alleged.htm>

(Accessed: 27 February 2018).

The National Archives (UK): CO 1035/117. Proposal to use information Research Department (IRD) material to counter Communist propaganda in colonies. January – December 1956.

The National Archives (UK): FCO 95/971. Nigeria Distribution of IRD material through Kaduna. 1970 Jan 01 - 1970 Dec 31.

The National Archives (UK): FO 1110/1961. Nigeria: scope of IRD work, proposal to temporarily second Field Officer to Kaduna and book reviews in local press. 1965 Jan 01 - 1966 Dec 31.

The National Archives (UK): FO 1110/1561. Latin America: information policy towards the area, IRD contribution and request for information about anti-Communist organisations active in Latin America. 1963 Jan 01 - 1963 Dec 31.

The National Archives (UK): FO 1110/182. Use of IRD material: use in Latin America. 1949.

The National Archives (UK): FCO 95/979. Colombia: distribution of IRD material. 1970 Jan 01 - 1970 Dec 31.

The National WW2 Museum (n.d.) *What Will Russia Do After the War?* Available at: <https://www.nationalww2museum.org/war/articles/what-will-russia-do-after-war> (Accessed: 1 November 2019)

The Washington Post (2015) *Full text: Obama's remarks on the killing of American held by al-Qaeda in a U.S. operation.* Available at: [https://www.washingtonpost.com/news/post-nation/wp/2015/04/23/full-text-obamas-remarks-on-the-killing-of-american-held-by-al-qaeda-in-a-u-s-operation/?noredirect=on&utm\\_term=.97002ba51aa0](https://www.washingtonpost.com/news/post-nation/wp/2015/04/23/full-text-obamas-remarks-on-the-killing-of-american-held-by-al-qaeda-in-a-u-s-operation/?noredirect=on&utm_term=.97002ba51aa0) (Accessed: 29 September 2018).

The Washington Post (2018) *The making of the Steele dossier.* Available at: [https://www.washingtonpost.com/graphics/2018/politics/steele-timeline/?noredirect=on&utm\\_term=.eaaf7dcb8f88](https://www.washingtonpost.com/graphics/2018/politics/steele-timeline/?noredirect=on&utm_term=.eaaf7dcb8f88) (Accessed: 1 June 2018).

The White Helmets (n.d.) *Support the White Helmets.* Available at: <https://www.whitehelmets.org/en> (Accessed: 11 November 2018).

The White House (n.d.) *Our Government: The Constitution*. Available at:

<https://www.whitehouse.gov/about-the-white-house/the-constitution/> (Accessed: 2 January 2020)

The White House (US) (2017), *Vulnerabilities Equities Policy and Process for the United States Government*. Available at:

<https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF> (Accessed: 20 December 2017).

Thomas, H. (2008) 'Cosmopolitanism', in Griffiths, M. (ed.) *Encyclopedia of International Relations and Global Politics*. London: Routledge, pp.138 – 141.

Thornton, S.W. (2000) 'Grief transformed: The mothers of the Plaza de Mayo', *OMEGA-Journal of Death and Dying*, 41(4), pp.279-289.

Treadwell, J. (2013) *Criminology: The Essentials*. 2<sup>nd</sup> edn. London: SAGE

Thucydides (2013) *The History of the Peloponnesian War*. Translated by Crawley, R. Available at: <http://www.gutenberg.org/files/7142/7142-h/7142-h.htm> (Accessed 2 November 2018).

Trend Micro (2017) *From Espionage to Cyber Propaganda: Pawn Storm's Activities over the Past Two Years*. Available at:

<https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/espionage-cyber-propaganda-two-years-of-pawn-storm> (Accessed: 7 July 2018).

Trump, D. (2019) [@RealDonaldTrump] *So interesting to see "Progressive" Democrat Congresswomen, who originally came from countries whose governments are a complete and total catastrophe, the worst, most corrupt and inept anywhere in the world (if they even have a functioning government at all), now loudly..... ..and viciously telling the people of the United States, the greatest and most powerful Nation on earth, how our government is to be run. Why don't they go back and help fix the*

*totally broken and crime infested places from which they came. Then come back and show us how.... it is done.* [Twitter] 14 July. Available at:

<https://twitter.com/realDonaldTrump/status/1150381396994723841> (Accessed: 2 November 2019)

Twitter Safety, (2019) *Information operations directed at Hong Kong*. Available at:

[https://blog.twitter.com/en\\_us/topics/company/2019/information\\_operations\\_directed\\_at\\_Hong\\_Kong.html](https://blog.twitter.com/en_us/topics/company/2019/information_operations_directed_at_Hong_Kong.html) (Accessed: 25 October 2019).

United Nations (n.d.[a]) *Human Rights Law*. Available at:

<https://www.un.org/en/sections/universal-declaration/human-rights-law/index.html> (Accessed: 3 January 2020)

United Nations (n.d.[b]) *Human Rights*. Available at: <https://www.un.org/en/sections/issues-depth/human-rights/> (Accessed: 30 November 2019).

United Nations (n.d.[c]) *Universal Declaration of Human Rights*. Available at:

<https://www.un.org/en/universal-declaration-human-rights/> (Accessed: 30 November 2019)

United Nations (n.d.[d]) *UN Charter (full text)*. Available at: <http://www.un.org/en/sections/un-charter/un-charter-full-text/index.html> (Accessed: 23 August 2018).

United Nations (2011) *Security Council Approves 'No-Fly Zone' over Libya, Authorizing 'All Necessary Measures' to Protect Civilians, by Vote of 10 in Favour with 5 Abstentions*. Available at: <https://www.un.org/press/en/2011/sc10200.doc.htm> (Accessed: 26 December 2018).

United Nations (2014) *68/167. The Right to Privacy in the Digital Age*. Available at:

<https://undocs.org/A/RES/68/167> (Accessed: 10 July 2018).

United Nations, (2016[a]) *The promotion, protection and enjoyment of human rights on the Internet*. Available at: <https://undocs.org/A/HRC/32/L.20> (Accessed: 12 December 2019)

United Nations (2016[b]) *Israel's Settlements Have No Legal Validity, Constitute Flagrant Violation of International Law, Security Council Reaffirms*. Available at: <https://www.un.org/press/en/2016/sc12657.doc.htm> (Accessed: 28 November 2018).

United Nations (2018[a]) *First Committee Approves 27 Texts, Including 2 Proposing New Groups to Develop Rules for States on Responsible Cyberspace Conduct*. Available at: <https://www.un.org/press/en/2018/gadis3619.doc.htm> (Accessed: 25 December 25, 2018).

United Nations (2018[b]) *In Emergency Meeting, Security Council Speakers Voice Grave Concern over Alleged Chemical Weapons Use in Syria, as Versions of Recent Attacks Sharply Differ*. Available at: <https://www.un.org/press/en/2018/sc13284.doc.htm> (Accessed: 12 June 2018).

United Nations Assistance Mission In Afghanistan (2018) *Highest Recorded Civilian Deaths From Conflict At Mid – Year Point – Latest UNAMA Update*. Available at: <https://unama.unmissions.org/highest-recorded-civilian-deaths-conflict-mid-year-point-latest-unama-update> (Accessed: 16 December 2018).

United Nations Economic and social Council, (2006) *PROMOTION AND PROTECTION OF HUMAN RIGHTS: Study on the right to the truth: Report of the Office of the United Nations High Commissioner for Human Rights*. Available at: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G06/106/56/PDF/G0610656.pdf?OpenElement> (Accessed: 21 November 2019)

United Nations High Commissioner for Refugees (2019) *Private Partners*. Available at: <https://www.unhcr.org/uk/private-sector-supporters.html> (Accessed: 15 April 2019).

United Nations News (2017) *Security Council fails at fresh attempt to renew panel investigating chemical weapons use in Syria*. Available at:



<https://news.un.org/en/story/2017/11/636602-security-council-fails-fresh-attempt-renew-panel-investigating-chemical-weapons#.WhWKKYXXLIU> (Accessed: 14 February 2018).

United Nations NEWS (2018) *Top UN judicial body orders US to ease Iran sanctions*. Available at: <https://news.un.org/en/story/2018/10/1022142> (Accessed: 28 November 2018).

United States Court (n.d.) *What Does the Fourth Amendment Mean?* Available at: <https://www.uscourts.gov/about-federal-courts/educational-resources/about-educational-outreach/activity-resources/what-does-0> (Accessed: 3 January 2020)

United States Department of Energy (n.d.[a]) *Espionage and the Manhattan Project*. at: <https://www.osti.gov/opennet/manhattan-project-history/Events/1942-1945/espionage.htm> (Accessed: 25 April 2018).

United States Department of Energy (n.d.[b]) *The Venona Intercepts*. Available at: <https://www.osti.gov/opennet/manhattan-project-history/Events/1945-present/venona.htm> (Accessed: 23th April 2018).

United States Department of Justice (n.d.[a]) *645. Entrapment—Elements*. Available at: <https://www.justice.gov/usam/criminal-resource-manual-645-entrapment-elements> (Accessed: 29 June 2018).

United States Department of Justice (n.d.[b]) *646. Recent Entrapment Cases*. Available at: <https://www.justice.gov/usam/criminal-resource-manual-646-recent-entrapment-cases> (Accessed: 29 June 2018).

United States Department of Justice (2014) *U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage*. Available at: <https://www.justice.gov/opa/pr/us-charges-five-chinese->

military-hackers-cyber-espionage-against-us-corporations-and-labor (Accessed: 11 December 2019)

United States Department of Justice Archives, (2017) *Undercover and Sensitive Operations Unit, Attorney General's Guidelines on FBI Undercover Operations, November 13, 1992*: Available at: <https://www.justice.gov/archives/ag/undercover-and-sensitive-operations-unit-attorney-generals-guidelines-fbi-undercover-operations#entrapment> (Access: 29 June 2018).

United States Department of Justice (2019) *WikiLeaks Founder Julian Assange Charged in 18-Count Superseding Indictment*. Available at: <https://www.justice.gov/opa/pr/wikileaks-founder-julian-assange-charged-18-count-superseding-indictment> (Accessed: 8 December 2019)

United States Department of State, (2001) *Psychological and Political Warfare*. Available at: [https://1997-2001.state.gov/about\\_state/history/intel/250\\_259.html](https://1997-2001.state.gov/about_state/history/intel/250_259.html) (Accessed: 15 June 2018).

United States Holocaust Memorial Museum, (n.d.) *Dr. Robert Ritter: Racial Science and "Gypsies"*. Available at: <https://www.ushmm.org/learn/students/learning-materials-and-resources/sinti-and-roma-victims-of-the-nazi-era/dr.-robert-ritter-racial-science-and-gypsies> (Accessed: 12 November 2019)

United States Holocaust Memorial Museum, (2003) *Propaganda slide entitled "The Jew a Bastard," illustrating different racial types, and characterizing Jews as a "bastard" race*. Available at: <https://collections.ushmm.org/search/catalog/pa1141741> (Accessed: 12 November 2019)

United States Holocaust Memorial Museum, (2014) *Nazi propaganda showing four disabled men*. Available at: <https://collections.ushmm.org/search/catalog/pa1146882> (Accessed: 12 November 2019)

United States Holocaust Memorial Museum, (2017) *Propaganda slide depicting friendship between an Aryan woman and a black woman as a loss of racial pride. The caption reads, "The result/Racial pride fades."* Available at:

<https://collections.ushmm.org/search/catalog/pa1067588> (Accessed: 12 November 2019).

United States Holocaust Memorial Museum, (2019) *Nazi propaganda film on eugenics.*

Available at: <https://collections.ushmm.org/search/catalog/irn1004798> (Accessed: 12 November 2019)

US Immigration and Customs Enforcement (2019) *8 individuals indicted for exploiting the US student visa system.* Available at: <https://www.ice.gov/news/releases/8-individuals-indicted-exploiting-us-student-visa-system> (Accessed: 18 May 2019).

‘United States Of America v. Abdella Ahmad Tounisi’ (2013) United States District Court Northern District Of Illinois Eastern Division, case 13 CR 0328. [Online]. Available at: [http://media1.s-nbcnews.com/i/MSNBC/Sections/NEWS/Tounisi\\_Complaint.pdf](http://media1.s-nbcnews.com/i/MSNBC/Sections/NEWS/Tounisi_Complaint.pdf) (Accessed: 29 September 2019).

‘United States of America v James Gonzalo Medina’ (2016) United States District Court for the Southern District of Florida, Case No. 16 [Online]. Available at: <https://www.justice.gov/opa/file/847996/download> (Accessed: 25 October 2019).

‘United States Of America v. Jorge Cortes’ (2014) United States District Court for the Southern District of California, case No. 12-50137 [Online]. Available at: <http://cdn.ca9.uscourts.gov/datastore/opinions/2014/03/17/12-50137.pdf> (Accessed 29 September 2018).

‘United States Of America v. Nicholas Michael Teasant’ (2014) United States District Court for the Eastern District of California, case 14-cr-087 JAM [Online]. Available at: <http://media1.s->

[nbcnews.com/i/MSNBC/Sections/NEWS/Teausant\\_Defense\\_Response\\_re\\_Bail\\_Motion.pdf](http://nbcnews.com/i/MSNBC/Sections/NEWS/Teausant_Defense_Response_re_Bail_Motion.pdf) (Accessed: 29 September 2018).

‘United States Of America v. PARK JIN HYOK’ (2018) United States District Court for the Central District of California, case No. MJ 18 – 1479 [Online]. Available at: <https://www.justice.gov/opa/press-release/file/1092091/download> (Accessed: 6 November 2019)

Université du Québec à Montréal (n.d.) *The IndoChina War: 1945-1956: An Interdisciplinary Tool*. Available at: <http://indochine.uqam.ca/en/historical-dictionary/1324-service-de-documentation-exteri-eure-et-de-contre-espionnage-sdece.html> (Accessed: 17 May 2020)

University of Virginia (2003) *Message to the Grass Roots Malcolm X*. Available at: <http://xroads.virginia.edu/~public/civilrights/a0147.html> (Accessed 28 June 2018).

University of Virginia (2007) *Buck v. Bell: The Test Case for Virginia’s Eugenic Sterilization Act*. Available at: <http://exhibits.hsl.virginia.edu/eugenics/3-buckvbell/> (Accessed: 12 November 2019)

Vallin, V.M. (2015) ‘France as the Gendarme of Africa, 1960–2014’, *Political science quarterly*, 130(1), pp. 79-101.

Van Damme, P. (2017) *DA to report Bell Pottinger to international PR bodies for unethical behaviour*. Available at: <https://www.da.org.za/2017/07/da-report-bell-pottinger-international-pr-bodies-unethical-behaviour/> (Accessed: 20 November 2019)

Van der Velden, L. (2015) ‘Leaky apps and data shots: Technologies of leakage and insertion in NSA-surveillance’, *Surveillance & Society*, 13(2), pp.182-196.

Van Puyvelde, D. (2014) ‘Intelligence, Democratic Accountability, and the Media in France’, *Democracy and Security*, 10(3), pp. 287-305.

Viotti, P.R and Kauppi, M.K. (2010) *International Relations Theory*. 4<sup>TH</sup> edn. New York: Longman.

Wagner, S. (2014) ‘Whispers from Below: Zionist Secret Diplomacy, Terrorism and British Security Inside and Out of Palestine, 1944–47’, *The Journal of Imperial and Commonwealth History*, 42(3), pp.440-463.

Wakefield, J. (2018) *TED 2018: Fake Obama video creator defends invention*. Available at: <https://www.bbc.co.uk/news/technology-43639704> (Accessed: 24 May 2019).

Waldman, P., Chapman, L. and Robertson, J. (2018) *Peter Thiel’s data-mining company is using War on Terror tools to track American citizens. The scary thing? Palantir is desperate for new customers*. Available at: <https://www.bloomberg.com/features/2018-palantir-peter-thiel/> (Accessed: 14 November 2019)

Wall Street Journal, (2015) *Obama Advocates for Gay Rights in Kenya*. Available at: <https://www.youtube.com/watch?v=ge25eYo2Z-Y> (Accessed: 20 November 2019).

Walsh, D. and Schleifer, T. (2016) *McCain: Russian cyberintrusions an ‘act of war’*. Available at: <https://edition.cnn.com/2016/12/30/politics/mccain-cyber-hearing/index.html> (Accessed: 21 May 2019).

Walton, C. (2017) *British Intel Files Reveal How the Zionist Stern Gang Terrorized London*. Available at: <https://www.haaretz.com/israel-news/.premium.MAGAZINE-british-intel-files-reveal-how-the-zionist-stern-gang-terrorized-london-1.5627474> (Accessed: 29 April 2020)

Waltz, K.N. (1986) ‘Anarchic Orders and Balances of Power’, in Keohane, R.O. (ed.) *Neorealism and Its Critics*. New York: Columbia University Press, pp. 98 – 130.

Waltz, K.N. (2004) 'Neorealism: Confusions and criticisms', *Journal of Politics and Society*, 15(1), pp.2-6.

Waltz, K.N. (2010) *Theory of International Politics*. Illinois: Waveland Press.

Waltzman, R. (2017) *The Weaponization of Information. The Need for Cognitive Security*. Available at: <https://www.rand.org/pubs/testimonies/CT473.html> (Accessed: 27 November 2018)

War Child (2018) *Our approach*. Available at: <https://www.warchild.org.uk/what-we-do> (Accessed: 11 November 2018).

Warner, (2008) Wanted: A Definition of "Intelligence": Understanding Our Craft. Available at: <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol46no3/article02.html#fn9> (Accessed: 14 December 2019)

Warner, M. (2018) *U.S. Sen. Mark R. Warner Transcript*. Available at: [https://carnegieendowment.org/files/2018-03-01\\_Warner%20Transcript.pdf](https://carnegieendowment.org/files/2018-03-01_Warner%20Transcript.pdf) (Accessed: 06 February 2019).

Webber, J. (2018) *Efraín Rios Montt, former Guatemala military dictator, dies aged 91*. Available at: <https://www.ft.com/content/f55ec5aa-35f3-11e8-8b98-2f31af407cc8> (Accessed: 2 November 2019)

Welch, D. (2013) *Propaganda Power And Persuasion*. London: The British Library.

Welch, D. (2014) *Depicting the enemy*. Available at: <https://www.bl.uk/world-war-one/articles/depicting-the-enemy> (Accessed 15 September 2018).

Welchman, G. (1986) 'From Polish Bomba to British Bombe: The birth of ultra', *Intelligence and National Security*, 1(1), pp. 71-110.

Wellcome Library (2019[a]) *Codebreakers: Makers of Modern Genetics: The Eugenics Society archive*. Available at: <https://wellcomelibrary.org/collections/digital-collections/makers-of-modern-genetics/digitised-archives/eugenics-society/> (Accessed: 12 November 2019)

West, N. (1988) *The Friends Britain's post war intelligence operations*. Available at <https://www.cia.gov/library/readingroom/docs/CIA-RDP96B01172R000100060001-5.pdf> (Accessed: 27 April 2020)

Wellcome Library, (2019[b]) *Posters: "Healthy Seed" and "Marry Wisely"*. Available at: <https://wellcomelibrary.org/item/b16239301#?c=0&m=0&s=0&cv=2&z=-0.8028%2C-0.0957%2C2.5824%2C1.6222> (Accessed: 12 November 2019)

Whelan, M.F. (1985) 'Lead us not into (unwarranted) temptation: A proposal to replace the entrapment defense with a reasonable-suspicion requirement', *University of Pennsylvania Law Review*, 133(5), pp.1193-1230.

White, R. (2008) 'Depleted uranium, state crime and the politics of knowing', *Theoretical Criminology*, 12(1), pp.31-54.

Williamson, E. (2019) *How Alex Jones and Infowars Helped a Florida Man Torment Sandy Hook Families*. Available at: <https://www.nytimes.com/2019/03/29/us/politics/alex-jones-infowars-sandy-hook.html> (Accessed: 1 January 2020)

WikiLeaks, (n.d.) *NSA Global SIGINT Highlights: US Spied On Japan's Secret WTO Plan*. Available at: [https://wikileaks.org/nsa-japan/intercepts/WikiLeaks\\_NSA\\_Spy\\_Japan\\_WTO\\_Plan.pdf](https://wikileaks.org/nsa-japan/intercepts/WikiLeaks_NSA_Spy_Japan_WTO_Plan.pdf) (Accessed: 17 May 2020)

WikiLeaks (2011) *Remote Monitoring & Infection Solutions*. Available at: [https://wikileaks.org/spyfiles/files/0/289\\_GAMMA-201110-FinSpy.pdf](https://wikileaks.org/spyfiles/files/0/289_GAMMA-201110-FinSpy.pdf) (Accessed: 28 September 28, 2018)

WikiLeaks (2017[a]) *Hillary Clinton Email Archive*. Available at: <https://wikileaks.org/clinton-emails/> (Accessed: 10 July 2018).

WikiLeaks (2017[b]) *Vault 7: CIA Hacking Tools Revealed*. Available at: <https://wikileaks.org/ciav7p1/> (Accessed: 10 July 2018).

Wilkin, B. (2014) *Aerial warfare during World War One*. Available at: <https://www.bl.uk/world-war-one/articles/aerial-warfare-during-world-war-one> (Accessed 26 October 2018).

Wilson Center (n.d.) *Korean War Biological Warfare Allegations*. Available at: <https://digitalarchive.wilsoncenter.org/collection/250/korean-war-biological-warfare-allegations> (Accessed: 27 February 2018).

Wilson Center (1948) *April 30, 1948 George F. Kennan on Organizing Political Warfare*. Available at: <https://digitalarchive.wilsoncenter.org/document/114320.pdf?v=944c40c2ed95dc52d2d6966ce7666f90> (Accessed: 11 July 2018).

Wilson Center (1952) *February 21, 1952 Cable, Mao Zedong to Filippov (Stalin)*. Translated by Kramer, M. Available at: <http://digitalarchive.wilsoncenter.org/document/123147.pdf?v=0de4379fd8e55415fbadd02b52031a41> (Accessed: 27 February 2018).

Wilson Center (1953[a]) *April 18, 1953 Explanatory Note from Lt. Gen. V.N. Razuvaev to L.P. Beria*. Translated by Weathersby, K. Available at: <http://digitalarchive.wilsoncenter.org/document/112026.pdf?v=f4a679b9a285e43d3c5efa211822fd97> (Accessed: 27 February 2018).

Wilson Center (1953[b]) *April 21, 1953 Memorandum from L.P. Beria to G.M. Malenkov and to the Presidium of the CC CPSU*. Translated by Weathersby, K. Available at:



<http://digitalarchive.wilsoncenter.org/document/112027.pdf?v=cd6f8af1834b3d71215d778840f85d9f> (Accessed: 27 Feb. 18).

Wilson Center (1953[c]) *April 14, 1953 Explanatory Note from Lieutenant Selivanov to L.P. Beria*. Translated by Weathersby, K. Available at:  
<http://digitalarchive.wilsoncenter.org/document/112025.pdf?v=534884b3dde9cb53d4c260530386d7ea> (Accessed: 27 February 2018).

Wilson Center (1956) *February 25, 1956 Khrushchev's Secret Speech, 'On the Cult of Personality and Its Consequences,' Delivered at the Twentieth Party Congress of the Communist Party of the Soviet Union*. Available at:  
<https://digitalarchive.wilsoncenter.org/document/115995.pdf?v=3c22b71b65bcbbe9fdfa9419c995> (Accessed: 8 April 2019).

Wilson Center (1997) *September, 1997 Wu Zhili, 'The Bacteriological War of 1952 is a False Alarm'*. Translated by Casey, D. Available at:  
<http://digitalarchive.wilsoncenter.org/document/123080.pdf?v=3312183f462f2491dab683d9e752c5ed> (Accessed: 27 February 2018).

Wilson Center (2011) *Did Stalin Lure the United States into the Korean War? New Evidence on the Origins of the Korean War*. Available at:  
<https://www.wilsoncenter.org/publication/did-stalin-lure-the-united-states-the-korean-war-new-evidence-the-origins-the-korean-war> (Accessed: 27 February 2018).

Williams, M.C. (2009) 'Waltz, realism and democracy', *International Relations*, 23(3), pp. 328-340.

Wohlforth, W.C. (2010) 'Realism' in Reus-Smit, C. and Snidal, D. (ed.)  
*The Oxford Handbook of International Relations*. Oxford: Oxford University Press, pp.131-149.

- Wolfe, P. (2006) 'Settler Colonialism and the Elimination of the Native', *Journal of genocide research*, 8(4), pp. 387-409.
- Wolfson, A. (2018) *Muhammad Ali lost everything in opposing the Vietnam War. But in 1968, he triumphed*. Available at: <https://eu.usatoday.com/story/news/2018/02/19/1968-project-muhammad-ali-vietnam-war/334759002/> (Accessed: 27 November 2019)
- Wong, S-L. (2019) *China masses troops in stadium near Hong Kong*. Available at: <https://www.ft.com/content/f52c298c-bf23-11e9-b350-db00d509634e> (Accessed: 2 January 2020)
- Wood, D.M. and Wright, S. (2015) 'Before and after Snowden', *Surveillance & Society*, 13(2), pp.132-138.
- Wright, J. (2017) 'The Turing Bombe Victory and the first naval Enigma decrypts', *Cryptologia*, 41(4), pp. 295-328.
- Yamaguchi, M. (2020) *Japanese Warship Heads to Middle East to Protect Tankers*. Available at: <https://apnews.com/cd195c12c643765466ea4d5925d07435> (Accessed: 18 May 2019)
- Young, J. (2017) 'Seeking ontological security through the rise of China: New Zealand as a small trading nation', *The Pacific Review*, 30(4), pp. 513-530.
- Zarakol, A. (2010) 'Ontological (In) security and State Denial of Historical Crimes: Turkey and Japan', *International Relations*, 24(1), pp. 3-23.
- Zarakol, A. (2016) 'States and ontological security: A historical rethinking', *Cooperation and Conflict*, 52(1), pp. 48-68.

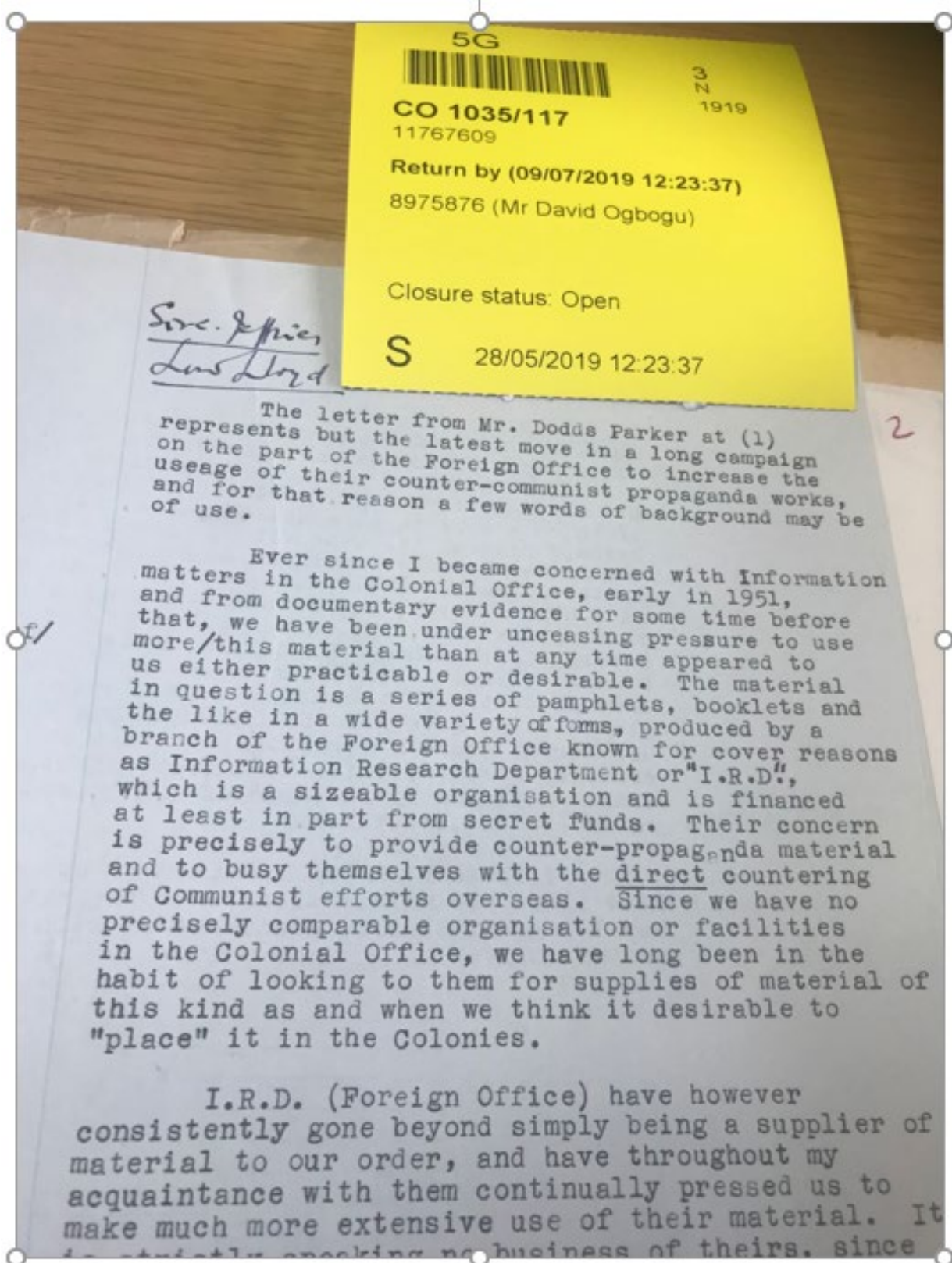
- ZeroHedge, (2019) *Iran Threatens To Close Key Oil Choke Point*. Available at: <https://oilprice.com/Geopolitics/International/Iran-Threatens-To-Close-Key-Oil-Choke-Point.html> (Accessed: 17 May 2020).
- Zetter, K. (2013) *How a Crypto 'Backdoor' Pitted the Tech World Against the NSA*. Available at: <https://www.wired.com/2013/09/nsa-backdoor/> (Accessed: 2 March 2019).
- Zhukova, E. (2016) 'From ontological security to cultural trauma: The case of Chernobyl in Belarus and Ukraine', *Acta Sociologica*, 59(4), pp. 332-346.
- Zollmann, F. (2017) 'Bringing Propaganda Back into News Media Studies', *Critical Sociology*, pp. 1-17.

---

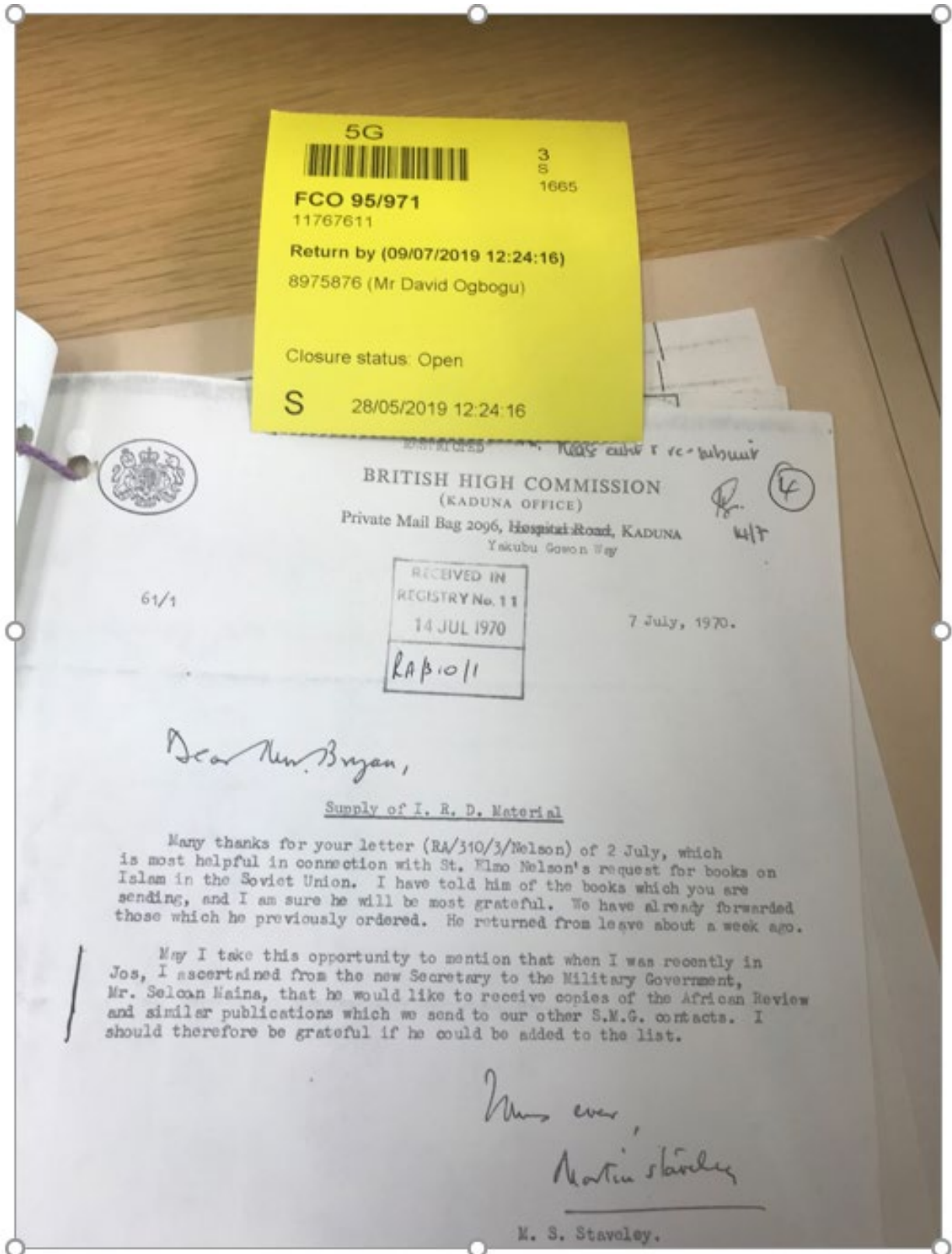
## Appendices

---

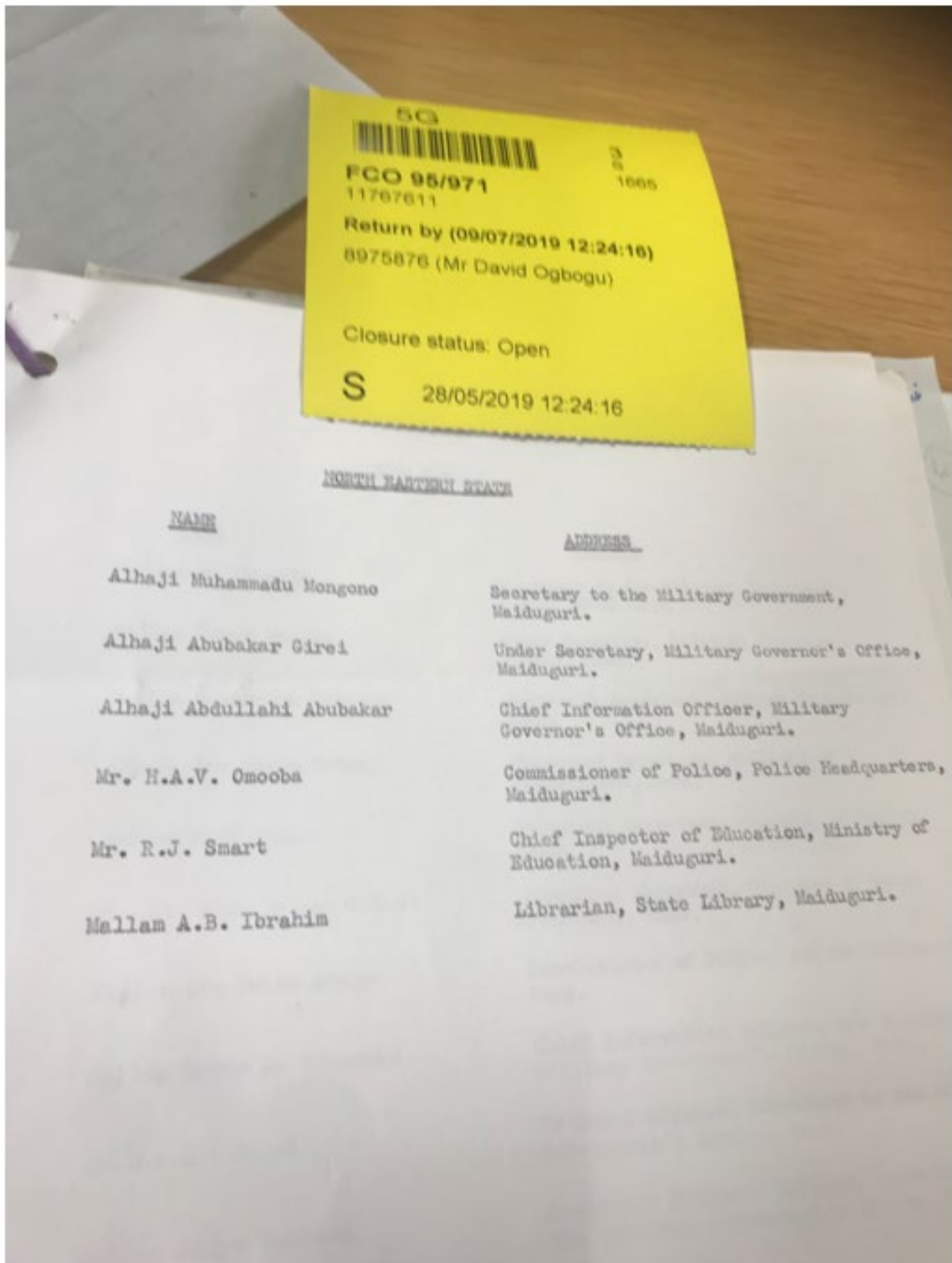
## Appendix 1: Snapshot of Information That Explains the Nature of the IRD



## Appendix 2: Snapshot of IRD Delivery of Books to Nigeria



### Appendix 3: Snapshot of IRD Contacts in Northern Nigeria



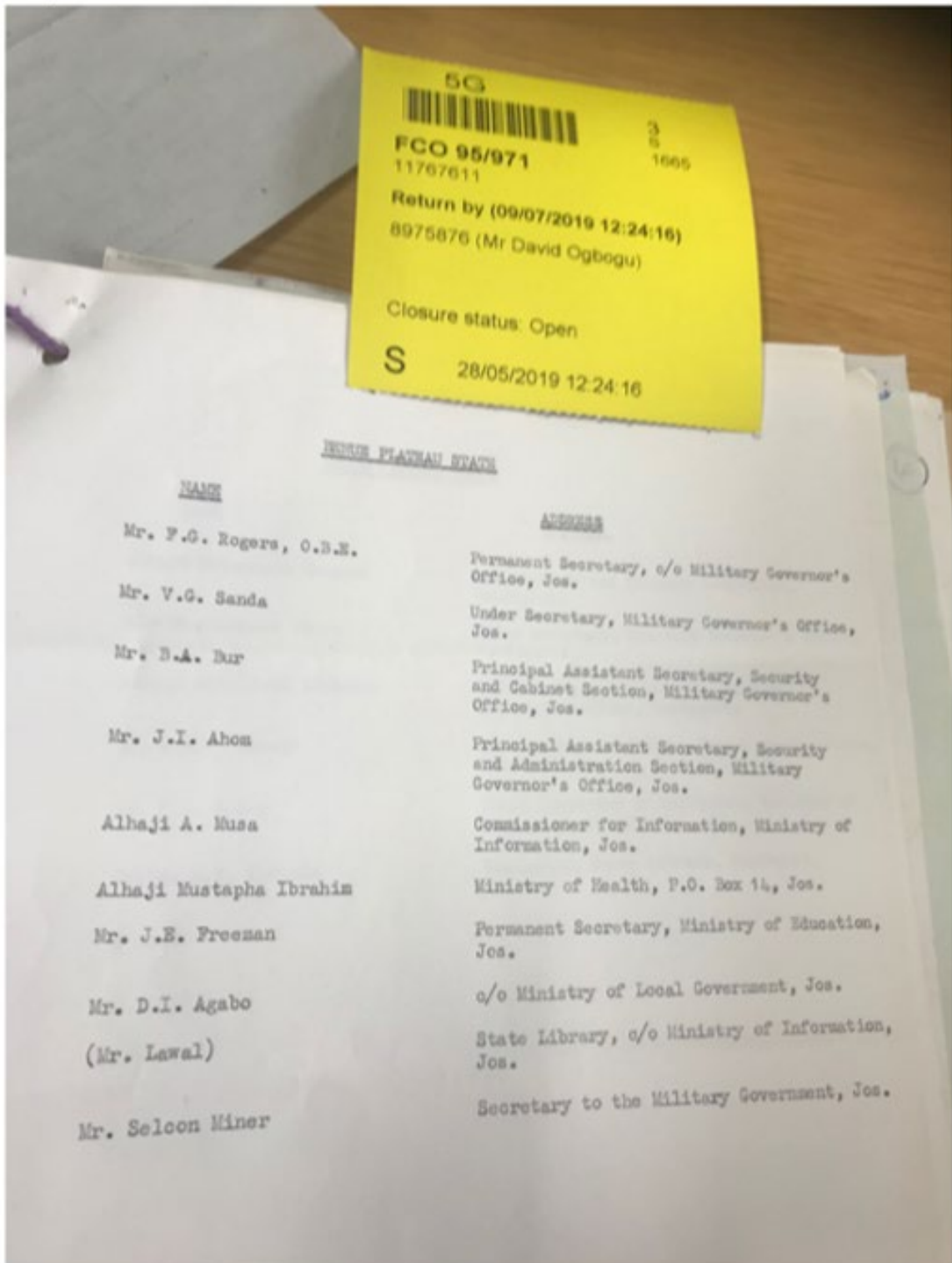
#### Appendix 4: Snapshot of IRD Contacts in Northern Nigeria

5G  
FCO 95/971  
11767611  
Return by (09/07/2019 12:24:16)  
8975876 (Mr David Ogbogu)  
Closure status: Open  
S 28/05/2019 12:24:16

KWARA STATE

<u>NAME</u>	<u>ADDRESS</u>
Alhaji A.L. Usaru	Secretary to the Military Government, Ilorin.
Mr. S.A. Adewusi	Commissioner of Police, Police Headquarters, Ilorin.
Mr. I.A. Obaro	Commissioner for Finance, Ministry of Finance, Ilorin.
Mr. A.A. Pejule	Commissioner for Works and Surveys, Ministry of Works and Surveys, Ilorin.
Mr. J.K. Bodunde	Chief Information Officer, c/o Military Governor's Office, Ilorin.
Mr. M. Ioka	Permanent Secretary, Ministry of Works and Surveys, Ilorin.
Mr. J.K. Salihu	Chief Inspector of Education, Ministry of Education, Ilorin.
Mr. J.O. Popoola	Librarian, Kwara State Library, Ilorin.
Mr. Emmanuel Adewumi	Protocol Officer, Military Governor's Office, P.M.B. 378, Ilorin.

### Appendix 5: Snapshot of IRD Contacts in Northern Nigeria



5G  
FCO 95/971  
11767611  
Return by (09/07/2019 12:24:16)  
8975876 (Mr David Ogbogu)  
Closure status: Open  
S 28/05/2019 12:24:16

NAME

ADDRESS

<u>NAME</u>	<u>ADDRESS</u>
Mr. F.G. Rogers, O.B.E.	Permanent Secretary, c/o Military Governor's Office, Jos.
Mr. V.G. Sanda	Under Secretary, Military Governor's Office, Jos.
Mr. B.A. Bur	Principal Assistant Secretary, Security and Cabinet Section, Military Governor's Office, Jos.
Mr. J.I. Ahom	Principal Assistant Secretary, Security and Administration Section, Military Governor's Office, Jos.
Alhaji A. Musa	Commissioner for Information, Ministry of Information, Jos.
Alhaji Mustapha Ibrahim	Ministry of Health, P.O. Box 14, Jos.
Mr. J.E. Freeman	Permanent Secretary, Ministry of Education, Jos.
Mr. D.I. Agabo	c/o Ministry of Local Government, Jos.
(Mr. Lawal)	State Library, c/o Ministry of Information, Jos.
Mr. Seloon Miner	Secretary to the Military Government, Jos.

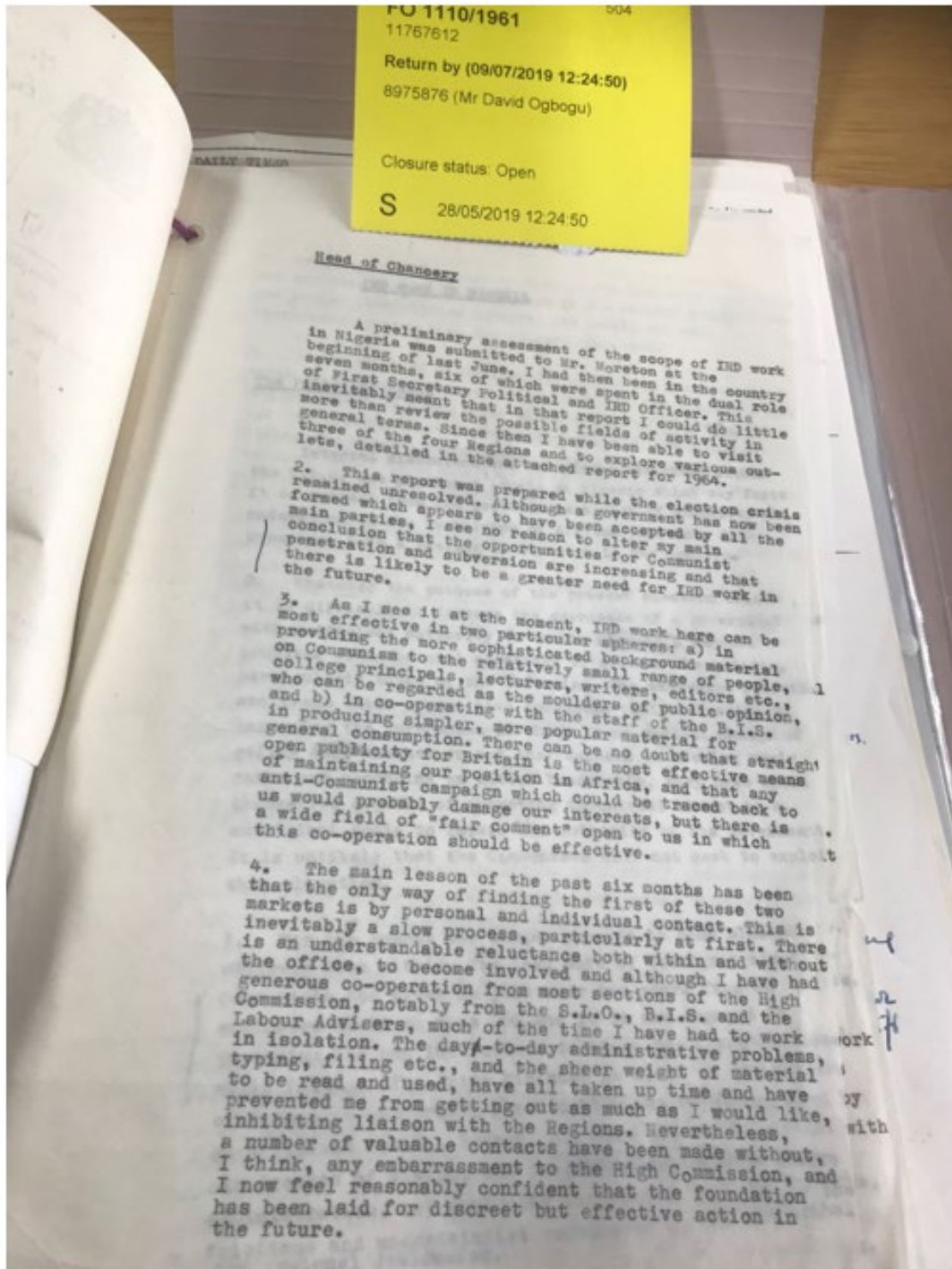


### Appendix 6: Snapshot of IRD Contacts in Northern Nigeria

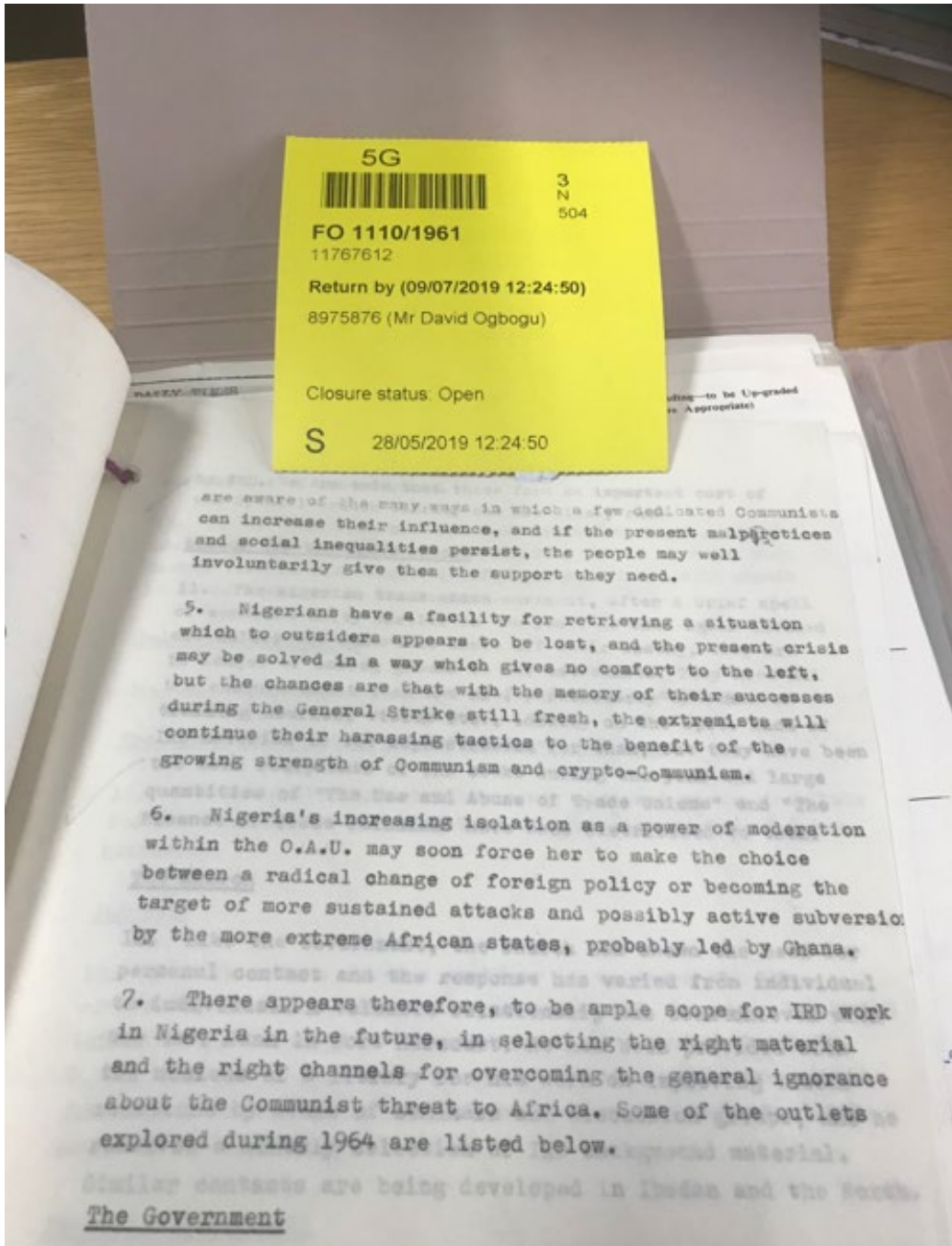
NORTH CENTRAL STATE

<u>NAME</u>	<u>ADDRESS</u>
<u>KADUNA</u>	
Alhaji Garba Ja Abdulkadir	Secretary to the Military Government, P.M.B. 2002.
Alhaji Baba Jimeta	Commissioner of Police, Police Headquarters.
Mr. E.D. Williams	Senior Principal Labour Officer, Federal Ministry of Labour Headquarters Office.
Father H. Bell	Regional Secretary, The Catholic Bishops' Education Council, P.O. Box 211.
Father Liam Burke	Secretary to the Catholic Archbishop, P.O. Box 14.
<u>ZARIA</u>	
Professor J. O'Connell	Head of Faculty of Government, Ahmadu Bello University.
Mr. J.M.M. Grey-Theriot	Librarian, Ahmadu Bello University
(Mrs. R.E.E. Young)	Deputy Librarian, Ahmadu Bello University.
Mr. Claude Scott	General Manager, Gaskiya Corporation.
Mr. A.J. Adeka	Department of Fine Art, Ahmadu Bello University.
Mallam Yakubu Adamu	Advanced Teachers' Training College, P.M.B. 1041.

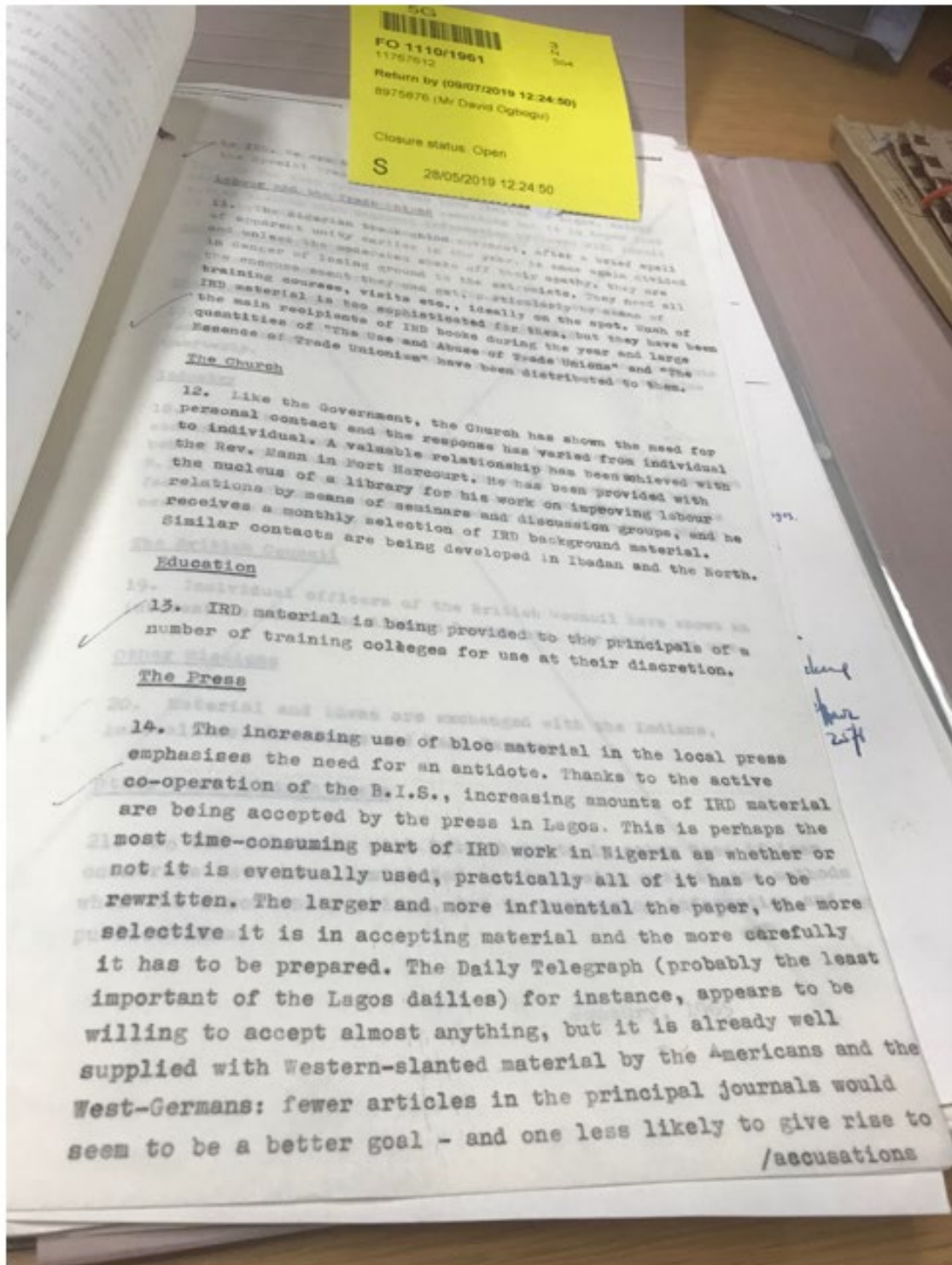
## Appendix 7: Snapshot of IRD Reflection Concerning Nigeria's Stability and Prospects



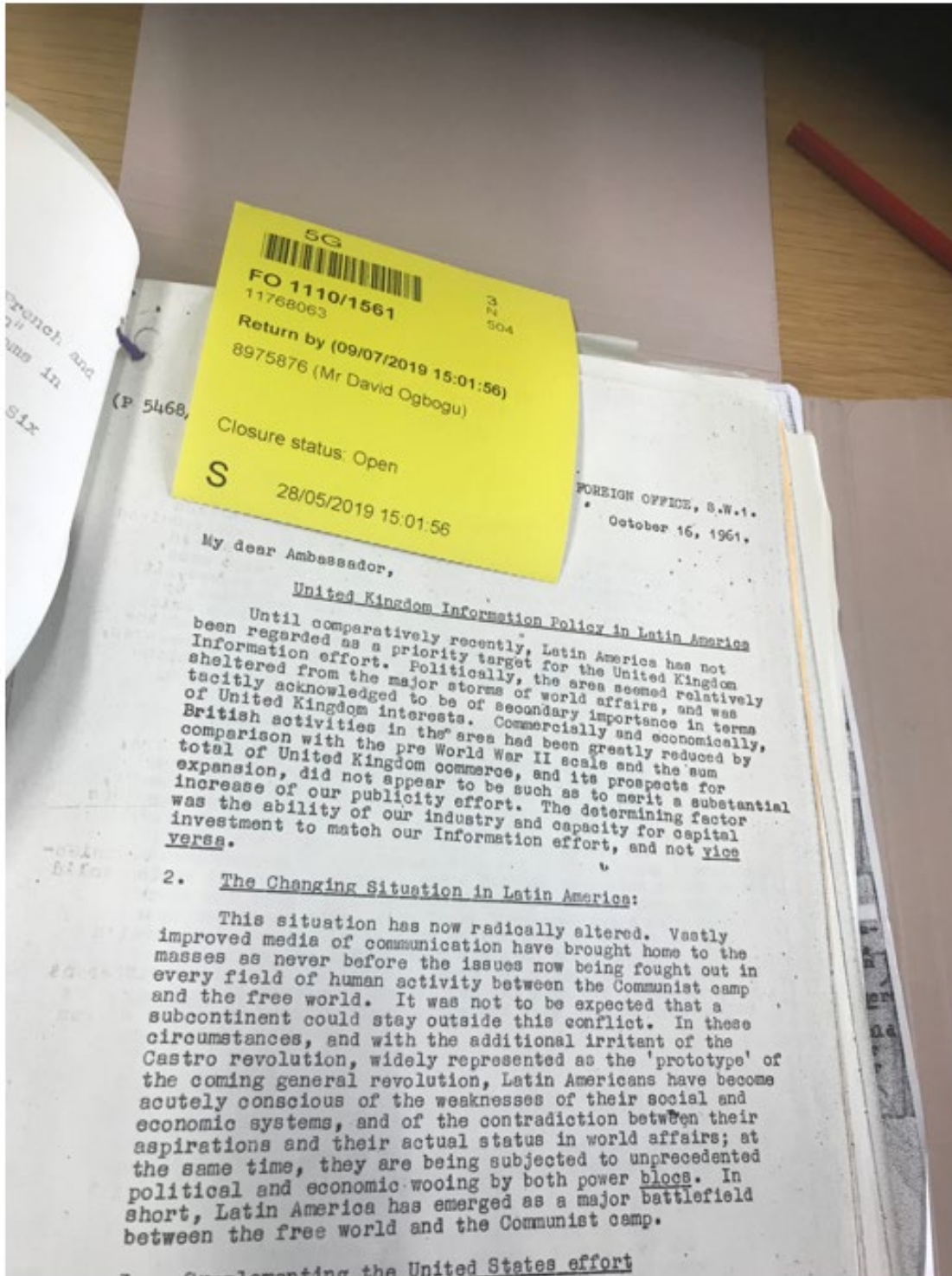
## Appendix 8: Snapshot of Foreign Office (IRD) Concerns about Threats of Subversion in Nigeria



Appendix 9: Snapshot of IRD Material in Nigeria's Press

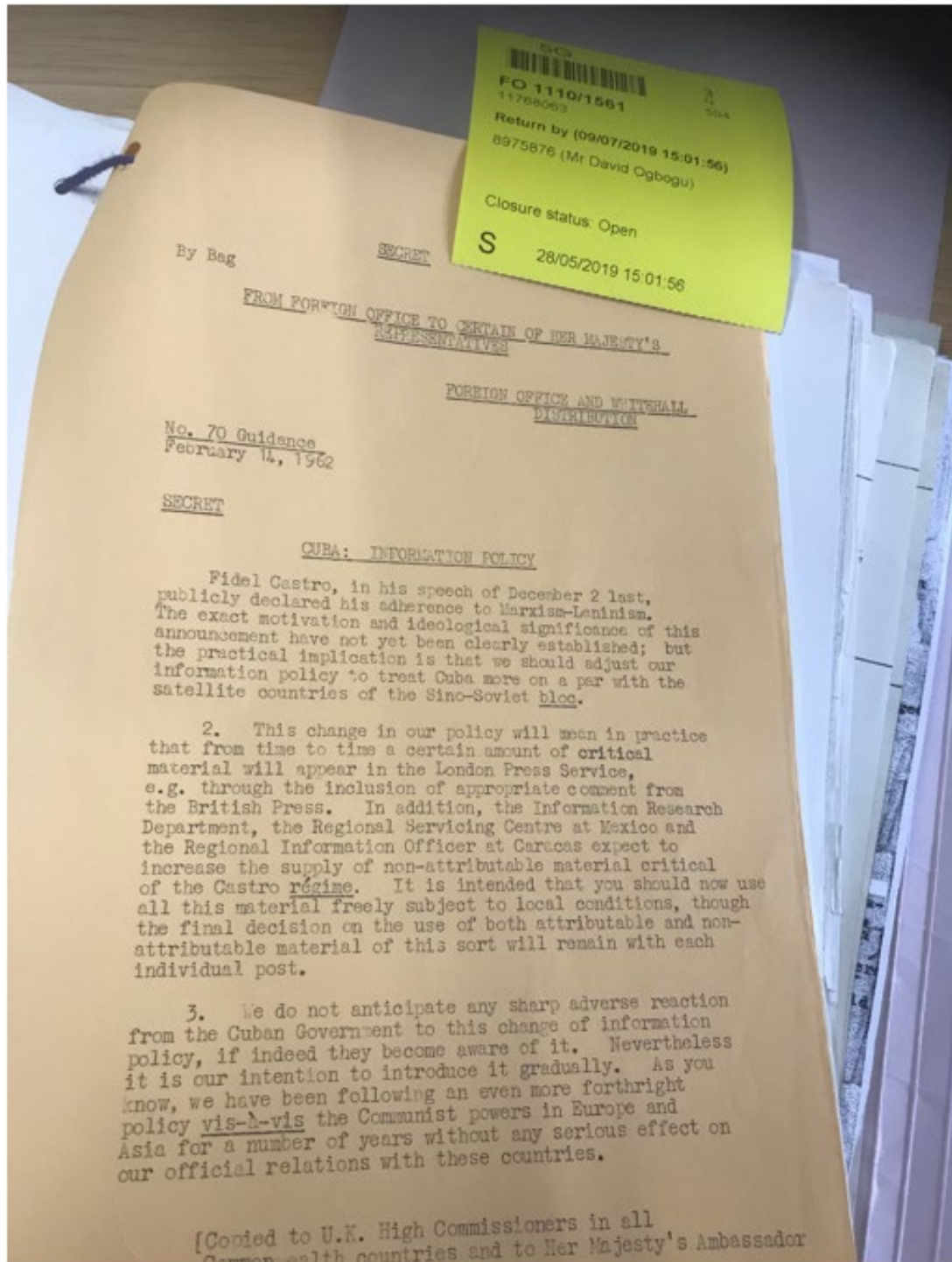


## Appendix 10: Snapshot of the UK Foreign Office Policy in Latin America

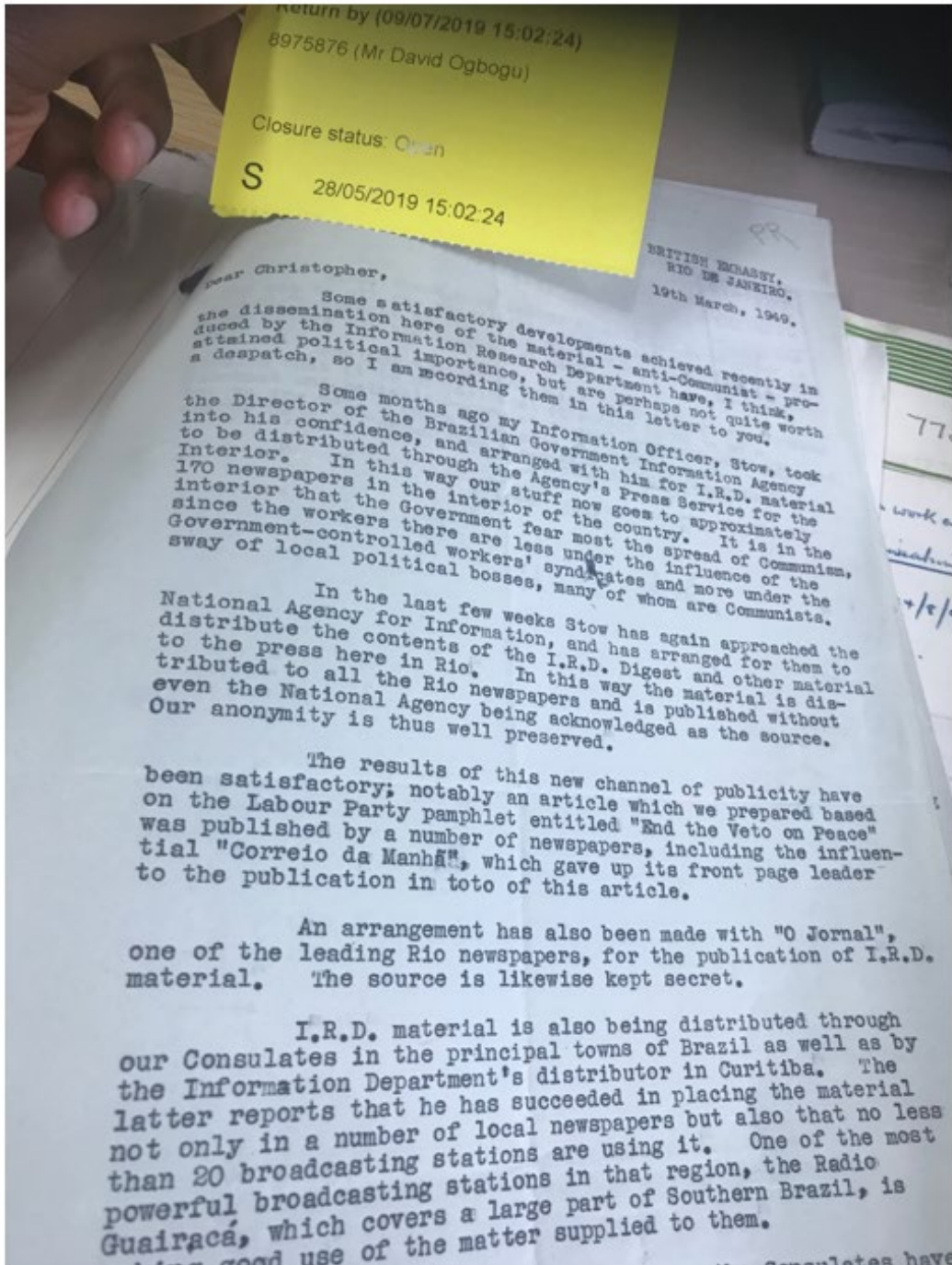




## Appendix 12: Snapshot of Foreign Office Information Policy towards Fidel Castro

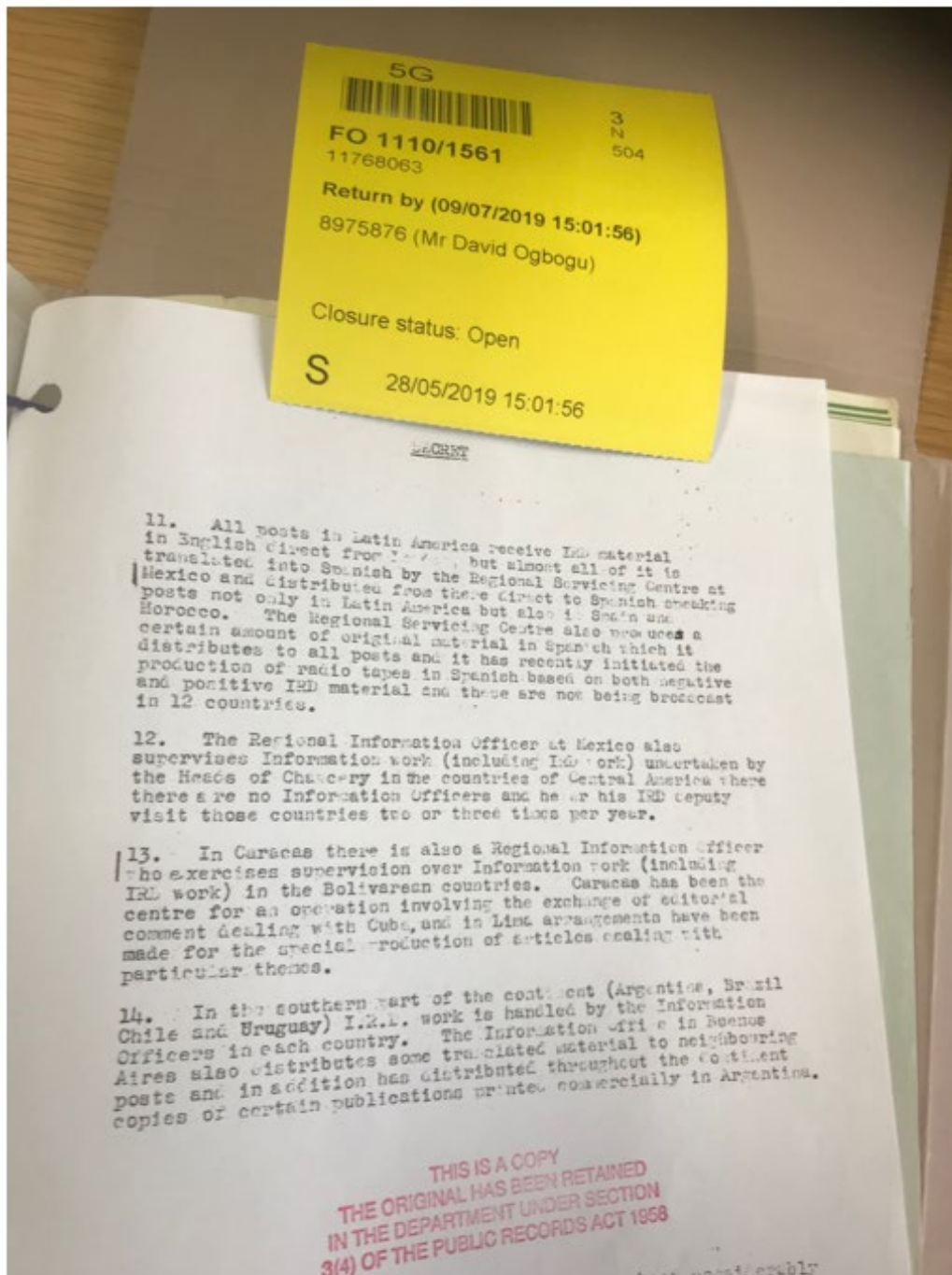


## Appendix 13: Snapshot of IRD Material in Latin America





## Appendix 14: Snapshot of IRD Material in Latin America's Media



## Ethics Form

### Section Applicant Details

<b>1.1 Details of Principal Investigator / Supervisor</b> <input type="checkbox"/> (tick as appropriate) <input type="checkbox"/>		
1.1a Name: Peter Hough	1.1b Department/role: Associate Professor	
1.1c Qualifications: PhD	1.1d Email: P.hough@mdx.ac.uk	1.1e Tel: 0208 4116034
<b>1.2 Details of Student Researcher (if applicable)</b>		
1.2a Name: David Emeka Ogbogu	1.2b Programme of study/module: MAIR Dissertation	
1.2c Qualifications: PhD	1.2d Email: Crossingtherubicon7@gmail.com	1.2e Tel:
<b>1.3 Details of any co-investigators (if applicable)</b>		
1.3a Name:	1.3b Organisation:	
1.3c Role:	1.3d Email:	
1.3e Name:	1.3f Organisation:	
1.3g Role:	1.3h Email:	
<b>1.4 Details of External Funding: N/A</b>		

### Section 2 – Details of proposed study



<b>2.1 Research project title:</b>	<b>Propaganda, Surveillance and Cyberspace: Consequences of Online Dirty Tricks</b>		
<b>2.2 Proposed start date</b>	February 2016	<b>2.3 Proposed end date</b>	August 2019
<b>2.4 Main aims of the study</b>			
<p>Amidst modern propaganda and surveillance campaigns in cyberspace that are wielded by intelligence services and non-state groups, are citizens capable enough to see through the schemes of nefarious actors online? Will society descend into what Walter Lippmann has described as a phantom public that is devoid of lucid thought and confidence to endure the modern cyber terrain? Furthermore, this research endeavours to appropriate the concept of Ontological (in) Security (OIS) in order to assess how states and citizens react towards online dirty tricks campaigns. I argue that state attempts to manage a Realist information environment with dirty tricks can lead to creating additional issues that produce OIS both domestically and abroad.</p>			
<b>2.5 Details of data collection procedures:</b> I obtained declassified information from the National Archives Centre. Moreover, I have obtained declassified files from the CIA, FBI and the Wilson Centre. However, I have used leaked information from reputable websites such as The Intercept and the Electronic Frontier Foundation. Investigative research from reputable organisations such as the Citizens Lab has been obtained and analysed.			

<b>Primary data collection.</b> <b>Secondary data analysis – See section 2.5!</b>		
Section 3 –Initial Checklist to be completed by all applicants	Yes	No
3.1 The research is <b>not empirical</b> (e.g., it is a theoretical discussion, review of existing literature, analytical and simulation modelling)	X	
3.2 The research involves <b>secondary data analysis*</b> where the researcher can provide evidence that they have the necessary <b>approval to access the data and DOES NOT involve access to records of personal or sensitive information concerning identifiable individuals, or internet research involving visual images or discussion of sensitive issues, or research which may involve sharing of confidential information beyond the initial consent given.</b>  <i>*Please provide evidence of approval. If there is data linkage or it may be otherwise possible to identify participants, please complete all sections of this form.</i>	X	
3.3 The research <b>already has ethical approval from another UK Ethics Committee</b> (e.g., HEI, NHS NRES) and the liability insurance is provided by the other body/institution*. <i>(Please provide evidence of approval)</i> *If MU liability sponsorship is required please complete all sections of this form.		-

If you have answered YES to any of the questions above, then **no further information is required**. Please go to and complete **Section 9** and sign the declaration in **Section 10**.

If you have answered NO to any of the questions above **please complete the remainder of this form for FULL ETHICS REVIEW**. (For research involving human tissue (including blood) please use the form and process for the Natural Sciences Department. For psychological research please use the forms and process for the Psychology Department.)

## Section 4 – Research Methods and Design |

<p>4.1 Please detail <b>ALL methods of data collection</b> for this research:</p>
<p>4.2 Will it be necessary for <b>participants to take part in the study without their knowledge and consent</b> at the time, e.g., covert observation?</p> <p><i>If 'yes', please provide justification and details of how this will be managed to respect the participants/third parties involved to respect their privacy, values and to minimise any risk of harmful consequences:</i></p>
<p>4.3 Will you <b>audio or video record</b> interviews and/or observations? Yes</p> <p><i>If 'yes' please provide details:</i></p>
<p>4.4 Will the research involve <b>respondents to the internet or other visual or vocal methods</b> where respondents may be identified?</p> <p><i>If 'yes' please provide details:</i></p>
<p>4.5 Will the research involve the <b>sharing of data or confidential information beyond the initial consent</b> given?</p> <p><i>If 'yes' please provide details:</i></p>
<p>4.6 How will you ensure compliance with the <b>Data Protection Act*</b> in terms of <b>anonymous data collection, maintaining confidentiality</b>, sharing and secure storage, through research dissemination plans and disposal of research data? (*see DPA checklist)</p>
<p>4.7 Will you use an <b>experimental research design</b> (ie., <a href="#">implement</a> a specific plan for assigning participants to conditions and noting consequent changes)?</p> <p><i>If 'yes', please provide details of treatment/intervention (and specify if these are intrusive interventions such as the use of hypnosis or physical exercise) and required resources:</i></p>
<p>4.8 Will the study involve <b>discussion of sensitive topics?</b> (e.g., sexual activity, drug use etc)</p> <p><i>If 'yes' please provide details:</i></p>
<p>4.9 Is <b>pain or more than mild discomfort</b> likely to result from the study?</p> <p><i>If 'yes' please provide details:</i></p>
<p>4.10 Could the study induce <b>psychological stress or anxiety or cause harm or negative consequences</b> beyond the risks encountered in normal life?</p> <p><i>If 'yes' please provide details:</i></p>
<p>4.11 <b>Avoiding harm</b> what has been done to assess, obviate or minimise potential risks and how will participants/third parties be supported?</p>

## Section 5 – Research Participants



5.1 Please indicate the **types of participants** that will be included in this research:

*(e.g., under 16yrs; patients; MU students; general public; specific group(s) or team(s); vulnerable adults unable to give informed consent\*etc.) \*All research that falls under the auspices of the Mental Capacity Act must be reviewed by NHS NRES.*

Specific person.

5.2 **Number of participants:** *(for each type of participant, if applicable)*

5.3 Briefly describe how **access** will be gained to participants: *(including details of access through gatekeepers, e.g., managers, parents)*

By telephone and email.

5.4 **Length of each data collection session, number of sessions and location of data collection** *i.e., will the study involve prolonged and repetitive testing? If so, please justify and state how participants will be supported? Short telephone interview.*

5.5 Does this research require **External Ethics Approval**?

*If 'yes' please provide details:*

## Section 6 – Safety and legal issues

6.1 Will you be **alone** with a participant or group of participants?

6.2 What **safety issues**\* does your methodology raise for you and for your participants and what mitigating actions will be taken?\*While researchers have a duty to not cause harm to participants, some research requires judgements to be made about what are acceptable/justifiable levels of harm in accordance with the potential benefits of the research. *If relevant to this research, please specify:*

6.3 What **legal issues** does your methodology raise for you and for your participants and what mitigating actions will be taken? *Please specify:*

6.4 Do you hold a current **Disclosure and Barring Service (DBS) Certificate**\*?

\*Needed when working with children or in healthcare.

**Section 7 – Research Collaboration**

7.1 Does the research involve an international collaborator or research conducted overseas? No  
 If 'yes', what ethical review procedures must this research comply with for that country, and what steps have been taken to comply with these:

Section 8 – Protocols for ethical research

	Yes	No
8.1 Will you ensure compliance with the <b>Data Protection Act?</b> (See DPA Checklist)		
8.2 Will you provide a <b>Participant Information Sheet</b> *?		
8.3 Will you obtain <b>Written Informed Consent</b> * directly from research participants?		
8.4 Will you obtain <b>Written Informed Consent</b> * directly from gatekeepers (if applicable)? N/A <input type="checkbox"/>		
8.5 Will you inform participants that their participation is <b>voluntary</b> and that they have a <b>right to withdraw</b> from the research at any time?		
8.6 Will you tell participants that their data will be treated <b>confidentially</b> and the limits of confidentiality will be made clear in your Participant Information Sheet?		
8.7 Will you inform participants of the limits of <b>anonymity</b> they will be afforded as participants? (e.g., their identities as participants will be concealed in all documents resulting from the research)		
8.8 Will you aim to <b>avoid harm</b> to your participants?		
8.9 Will you ensure your research is <b>independent and impartial</b> ?		
8.10 Will you provide a <b>Written Debriefing Sheet</b> *? (if applicable)N/A <input type="checkbox"/>		

\*Please submit copies of these forms with this application

If you have answered **No** to any of the questions above, please explain below:

Section 9: Other Ethical Issues – to be completed by all applicants

Does the study involve any **other ethical issues** not covered above?

*If 'yes' please give details:*

### Section 10: Declaration – to be completed by all applicants

Applicants should read and sign the following declaration before submitting the application.

**Please ensure that you have read and understood the relevant Code(s) of Ethics appropriate to your research field and topic.**

**In signing this research ethics declaration I am confirming that:**

1. I have read and understood the relevant Code(s) of Ethics appropriate to my research field and topic.
2. The research ethics application form is accurate to the best of my knowledge and belief.
3. I have read and understand the University's *Code of Practice For Research: Principles and Procedures*
4. I agree to abide by the research ethics applicable to the project and which are listed above.
5. I understand that it is my responsibility to ensure that the research is conducted in accordance with my professional/statutory/regulatory body Code of Conduct/Code of Ethics/Research Governance Framework.
6. There is no potential material interest that may, or may appear to, impair the independence and objectivity of researchers conducting this project.
7. I have received and will submit evidence of authorisation from the relevant authorities to carry out the research with this application – if applicable.
8. I agree to inform my Supervisor/School/Institute or Departmental Research Ethics Committee of any adverse effects.
9. I understand that the project, including research records and data, may be subject to inspection for audit purposes at any time in the future.
10. I understand that personal data about me contained in this form will be held by those involved in the ethics approval procedure and that it will be managed according to Data Protection Act principles.
11. I will notify my Supervisor/School/Institute or Departmental Research Ethics Committee of any proposed changes to this methodology.
12. I have seen and signed a risk assessment for this research study.

**For supervisors:**

1. I confirm that I have reviewed all the information submitted with this research ethics application.
2. I also accept responsibility for guiding the applicant so as to ensure compliance with the terms of the protocol and with any applicable Code(s) of Ethics.
3. I understand that research/data may be subject to inspection for audit purposes and I agree to participate in any audit procedures required by the University Ethics Committee (UEC) if requested.
4. I confirm that it is my responsibility to ensure that students under my supervision undertake a risk assessment to ensure that health and safety of themselves, participants and others is not jeopardised during the course of this study.

5. I have seen and signed a risk assessment for this research study (if applicable).

Signature: Principle Investigator/Supervisor

.....  .....

Print name: .....Dr Peter Hough.....

Date: .....14/12/2018..... (dd/mm/yyyy)

Student's signature (if applicable):

.....David Emeka Ogbogu.....

Print name: David Emeka  
Ogbogu.....

Date: ..... 14/12/2018..... (dd/mm/yyyy)