Covert Action and Cyber Offensive Operations: Revisiting Traditional Approaches in Light of New Technology

WILLIAM ROBERT CARRUTHERS

Submitted in Partial Fulfilment of the Requirements of the Degree of Doctor of Philosophy

University of Salford,
School of Arts and Media

2018

TABLE OF CONTENTS

Figure List

Acknowledgments

The author would like to thank his supervisory team Dr Samantha Newbery and Professor Alaric Searle without whom this would not have been possible.

The author would also like to thank the Snowden Surveillance Archive, Edwardsnowden.com, and the National Security Archive for allowing people to access documents online free of charge.

Finally the author would like to thank his family for helping him throughout the Ph.D, especially Andrea Carruthers who helped him so much to cross the finishing line with the thesis.

Abstract

Over the last three years a number of significant, alleged cyber offensive operations have taken place: the North Korean operations against Sony Pictures in 2014; the BlackEnergy3 Virus which targeted Ukrainian power substations in 2015; and the cyber offensive operations that were designed to influence recent presidential elections. This thesis will investigate whether these types of operations are new or similar to activities that took place in the twentieth century, especially during the Cold War, termed 'covert action'. Focusing on the US and British experience, and using a comparative methodology, this study will compare covert action and cyber offensive operations. It will achieve this by addressing what covert action is and what forms it takes; this will then be employed in the analysis of cyber offensive operations. The thesis seeks to establish a clear relationship between these two forms of state tactics employed against state and non-state actors. It argues that although the two forms of behaviour are linked, there is a need to modify the existing understanding of covert action; this will allow, in turn, a clearer understanding of the nature of cyber offensive operations to be developed. It is concluded that there is a need to re-examine the organisational structures of covert action, including ethical dimensions, in relation to cyber operations.

Introduction

The aim of this thesis is to establish if there is a relationship between covert action and cyber operations. If such a relationship exists, the thesis will seek to understand it. Covert action is defined as 'an activity or activities … to influence political, economic, or military conditions abroad where the role of the … government will not be apparent or acknowledged publicly'.[1] It has been argued that covert action is used outside of a war.[2] 'Cyber operations' according to the United States of America (US) government is a collective term referring to cyber intelligence (cyber espionage), offensive use of cyber operations, and cyber defence (defence against intelligence gathering and cyber offensive operations).[3] However this thesis will focus on the offensive use of cyber operations that the US defined as Offensive Cyber Effects Operations (OCEO). It was argued by the US that OCEO were

> operations and related programs or activities – other than network defense, cyber collection or Defense Cyber Effects Operations (DCEO) – conducted by or on behalf of the United States Government, in or through cyberspace, that are intended to enable or produce cyber effects outside United States Government networks.[4]

The British signals intelligence agency, the Government Communications Headquarters (GCHQ) used a similar term to define offensive use of cyber operations although they term them 'cyber effects operations'. These operations are, according to GCHQ, based on the idea that they 'produce effects in the real world'.[5] This document, however, did not explain what was meant by 'produce effects in the real world'. It could be that it means that instead of simply monitoring the cyber world, these operations are designed to produce a change that has consequences that can be

[1] Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, Fourth Edition (Washington, DC: CQ Press, 2009), p. 165.
[2] Ibid., p. 165.
[3] This document was leaked by Edward Snowden., all document that were leaked by Edward Snowden will herein be referred to as 'Edward Snowden Document'. All these leaked documents have been accessed either via the Snowden Surveillance Archive https://snowdenarchive.cjfe.org/greenstone/cgi-bin/library.cgi?e=q-00100-00---off-0snowden1--00-2----0-10-0---0---0direct-10-and%2cand%2cand-TE%2cTT%2cDE%2cSU--4--law%2c%2c%2c-----0-1l--00-en-50---50-about-TE%3a%28law%29--01-3-1-00-00--4--0--0-0-01-10-0utfZz-8-00&a=p&p=about or edwardsnowden.com https://search.edwardsnowden.com/ unless otherwise stated. Edward Snowden Document, US Government, 'Presidential Policy Directive/PPD-20 Subject US Cyber Operations Policy', no date given, p. 3 accessed via edwardsnowden.com.
[4] Edward Snowden Document, US Government, 'Presidential Policy Directive/PPD-20 Subject US Cyber Operations Policy', n.d., p. 3, edwardsnowden.com.
[5] Edward Snowden Document, GCHQ, 'Full Spectrum Cyber Effects SIGINT as an Enabler for GCHQ's 'Effects' Mission', ca.2010, p. 3, Snowden Surveillance Archive.

seen. Due to the fact that both the US and the GCHQ definitions of the operations fail to account for what is meant by an effect, this author has chosen instead to term these as ‘cyber offensive operations’.

This thesis will concentrate on cyber offensive operations. It seeks to differentiate cyber offensive operations from cyber intelligence. Cyber intelligence is about gathering information whereas cyber offensive operations are designed to cause a change. In some ways, a change can be produced by intelligence in the sense that intelligence is used to make policy which, to some extent, could lead to a change. However, the difference is that cyber intelligence produces a change in an indirect manner, whereas cyber offensive operations produce a change as a direct consequence of the operation. The reason to make a clear distinction is that both types of operations can use similar techniques. For example, breaking into an organisation’s systems can be used to gather intelligence by looking at or extracting documents, information, or data that is contained within the systems, but, if this operation was to be used to change documents, then this would be cyber offensive because it is looking to cause a change.

Furthermore, the term ‘cyber offensive’ is used here instead of ‘attack’. An attack implies that an operation will be directed through actions such as hacking, or through the use of malware. Malware is software that is introduced into a computer system that alters the way a computer or a system works. Cyber offensive operations, however, as will be show below, do not have to be conducted using these techniques; they may be used in some operations but are not limited to introducing malware. For example, as will be shown in chapter two, cyber offensive operations can be used to spread propaganda. This type of activity does not have to utilise malware but it can still produce a change. From this then, what makes a cyber offensive operation is that the operation is being conducted with the objective that it will produce a change. Finally, this study will not examine in detail the technological aspects of cyber other than that which is necessary to outline an operation.

The thesis will also seek to understand the ways that the US and the United Kingdom (UK) are using and could use cyber offensive operations. Firstly, with the leaking of information from Edward Snowden there is now new evidence about these organisations. Edward Snowden was a former contractor for the US signals intelligence agency the National Security Agency (NSA). In 2013, he stole a large

number of documents relating to the NSA and other intelligence agencies from both US and international organisations and has released a large number of these documents into the public domain. Secondly, the US and the UK were the founding members of what has become known as the 'Five Eyes' intelligence partnership. The 'Five Eyes' is now comprised of the US NSA, the UK GCHQ, Australian Signals Directorate (ASD), Canada's Communications Security Establishment (CSE), and New Zealand's Government Communications Security Bureau (GCSB). This partnership was created after the Second World War and governed the collection of signals intelligence. It has been argued that this relationship has 'created a global multilateral alliance' which in turn has 'almost unlimited intelligence power'.[6] This has meant that, with the documents that were leaked by Edward Snowden, there is now new evidence that is critically important in helping to understand cyber offensive operations. However, this author will focus on the UK and the US, due to the fact that they feature heavily within the leaked documents relating to cyber offensive operations. When assessing the US and UK's use of cyber offensive operations, the thesis will also examine some of the operations that other states have conducted to allow for a greater understanding of cyber offensive operations.

There is also evidence from public documents that provides some details of the development of cyber offensive operations in the US and UK. In the US, the fact of a military involvement with cyber offensive operations can be seen through the creation of US Cyber Command. This was created in 2009 and became fully operational in 2010. It is comprised of cyber units from four parts of the US Department of Defense: Army Cyber Command (ARCYBER), Fleet Cyber Command (FLTCYBER), Air Force Cyber Command (AFCYBER) and Marine Forces Cyber Command (MARFORCYBER).[7] It also works in conjunction with US Coast Guard Cyber Command (CGCYBER), which is technically part of the Department of Homeland Security. In addition, the US Department of Defense has argued that it 'has developed capabilities for cyber operations and is integrating those capabilities into the full array of tools that the United States government uses to defend U.S. national

[6] Richard J. Aldrich, *GCHQ: The Uncensored Story of Britain's Most Secret Intelligence Agency* (London: Harper Press, 2011), p. 89.
[7] Jean-Loup Samaan, 'Cyber Command', *The RUSI Journal*, 155:6, (2010), 16-21, 16.

interests'.[8] Further, their strategic goals include to 'build and maintain ready forces and capabilities to conduct cyberspace operations'[9] and to 'build and maintain viable cyber options and plan to use those options to control conflict escalation and to shape the conflict environment at all stages'.[10] The Department of Defense stated that they will establish a Cyber Mission Force that will eventually employ around 6,200 personnel.[11] These personnel will be divided into 133 teams with a range of objectives including cyber defence and cyber offensive operations.[12] The Department of Defense argue that they will be 'applying Cyber Mission Force capabilities more broadly'.[13] The Department of Defense has stated that twenty-seven of the 133 teams will be dedicated to what they term 'Combat Mission Teams' that will 'provide support to Combatant Commands by generating integrated cyberspace effects in support of operational plans and contingency operations'.[14] In this statement, the question must be what constitutes contingency operations. As it has stated that they will be used for military operations, this may mean that contingency operations might not be military operations themselves. What this something else is, it must be noted, is unclear from the statement but it could be argued that it means US Cyber Command would be used for operations outside a military situation. This is because the term 'operational plans' indicates a military use so it must be seen that it will be used outside a military context. In this way it could be argued that from these documents there is clear evidence that the US have developed the use of cyber offensive operations for operations which are interlinked with covert action. As they are looking to cause a change of behaviour, they are conducting the operations covertly, and they are being used outside of a military operation.

In addition to this, it can also be seen, from the files that have been leaked by Edward Snowden, there is further evidence of the planning and the policy directed

[8] US Government, Department of Defense, 'The Department of Defense Cyber Strategy', April 2015, p. 2.
[9] Ibid., p. 7.
[10] Ibid., p. 8.
[11] US Government, Department of Defense, 'Fact Sheet: The Department Of Defense Cyber Strategy', April 2015, p. 1.
[12] US Government, Department of Defense, http://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy.
[13] US Government, Department of Defense, 'Cybercom Chief Details Strategic Priorities for 2016', http://www.defense.gov/News-Article-View/Article/643954/cybercom-chief-details-strategic-priorities-for-2016, last accessed on 25.01.2016.
[14] US Government, Department of Defense, http://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy.

towards the use of offensive cyber capabilities. In a document that was written by the NSA, there are clear indications that they were involved in the development of cyber offensive operations. This can be seen in a file where it argues that the NSA was looking for an intern 'who likes to break things'.[15] As such they were looking for someone who could 'remotely degrade or destroy opponent computers, routers, servers and network enabled devices by attacking the hardware using low-level programming'.[16] The development of cyber offensive operations can be seen further through the 'Presidential Policy Directive/PPD-20 Subject US Cyber Operations Policy'. Within this document, there are a number of important points that must be taken into account:

> The United States has an abiding interest in developing and maintaining use of cyberspace as an integral part of US national capabilities to collect intelligence and to deter, deny, or defeat any adversary that seeks to harm US national interest in peace, crisis, or war.[17]

This shows that cyber offensive operations can be outside of a military context as it has argued that they could be used in war but also in peace and crisis. Also, with the terms 'deny and defeat' this then shows an ability to use cyber powers in an offensive capacity. Furthermore, this document also argued that:

> The United States Government shall conduct all cyber operations consistent with the US constitution and other applicable laws and policies of the United States, including Presidential orders and directives…This directive pertains to cyber operations, including those that support or enable kinetic, information, or other types of operations.[18]

This clearly shows that, in the terms of the US, a policy has been developed within which they could use their cyber offensive operations. Under the definitions section of the document it is clear that the US government's thinking was directed towards the use of cyber offensive operations. This is because they argued that this directive means that 'the United States Government shall conduct DCEO and OCEO'.[19] Within this document, it is also stated that the term cyber effects means that to the US government, this is at least: 'The manipulation, disruption, denial, degradation, or destruction of computers, information or communication systems, networks, physical

[15] Edward Snowden Document, NSA, 'S3285/ Intern Projects' 08.01.2008, p. 2, Snowden Surveillance Archive
[16] Ibid., p. 2.
[17] Edward Snowden Document, US Government, 'Presidential Policy Directive/PPD-20 Subject US Cyber Operations Policy', n.d, p. 4, edwardsnowden.com.
[18] Ibid., p. 4.
[19] Ibid., p. 3.

or virtual infrastructure controlled by computers or information systems, or information resident thereon'.[20] This then shows that they are considering using cyber for operations that are not just military in nature. Furthermore, with the terms 'manipulation', 'disruption', 'denial', 'degrade' and 'destruction', it shows that the US has looked to use cyber for offensive operations. This is because it is a move away from the collection of intelligence, thus suggesting an offensive use. This provides further evidence to show that the US government has developed a policy of using cyber offensive operations.

It can also be seen that it is not only the US that have developed a policy of using cyber offensive operations. The British government has developed a policy where it can be seen that they will use cyber offensive capabilities to achieve objectives. The Intelligence and Security Committee, the UK's main intelligence oversight body, suggested in its 2012 annual report that the UK has developed a policy of using cyber for offensive operations. The Committee argued that

> while attacks in cyberspace represent a significant threat to the UK, and defending against them must be a priority, we believe that there are also significant opportunities for our intelligence and security agencies and military which should be exploited in the interests of UK national security.[21]

Further in 2013, the Committee argued that the UK should use more proactive cyber capabilities that are closely linked to defence.[22] How the Committee felt that cyber offensive operations could be used in the future can be seen in their 2012 report. The committee provided a list of ways that cyber operations could be used, including active defence and cyber intelligence.[23] They then argued for, what could be seen as, cyber offensive operations. They felt that these could be: firstly, 'disruption' which was defined as 'accessing the networks or systems of others to hamper their activities or capabilities without detection (or at least without attribution)'; secondly, 'information operations using cyber techniques and capabilities in order to deliver information operations'; and finally as, 'military effects the destruction of data,

[20] Ibid., p. 2.
[21] HM Government, Intelligence and Security Committee, 'Annual Report 2011–2012', published July 2012, p. 35.
[22] HM Government, Intelligence and Security Committee, 'Annual Report 2012-2013', published July 2013, p. 20.
[23] HM Government, Intelligence and Security Committee, 'Annual Report 2011–2012', published in July 2012. p. 36.

networks or systems in support of armed conflict'.[24] In 2016 the UK government added further evidence about how Britain could use these operations. They stated that 'offensive cyber capabilities involve deliberate intrusions into opponents' systems or networks, with the intention of causing damage, disruption or destruction'.[25] They argued that they would 'have at our disposal appropriate offensive cyber capabilities that can be deployed at a time and place of our choosing, for both deterrence and operational purposes, in accordance with national and international law'.[26] In these ways, it is clear that Britain had begun to envision the use of cyber offensive operations and had given consideration to how they could be conducted.

The leaked documents from Edward Snowden provide further evidence to show that the UK government has developed the use of cyber offensive operations. This can be seen in the fact that GCHQ stated that they conduct effects operations. These operations have the basis of 'Destroy, Deny, Degrade, Disrupt, Deceive, Protect'.[27] These then have the objective of 'having an impact in the real world'.[28] Furthermore, GCHQ have stated that these types of operations amount to around five per cent of the operations that they undertake (how these operations are used will be discussed in chapters two, three, and four).[29] In this file, GCHQ argued that there are a number of operations that can be conducted with various goals ranging from low-end effects to conducting operations to target critical national infrastructure. In another document leaked by Snowden, it is shown that GCHQ, under the control of the Joint Threat Research Intelligence Group (JTRIG), has a database of tools that they have developed to be used for what could be argued are cyber offensive operations.[30] This group stated that they could develop other capabilities as needed to achieve missions.[31] This document makes it clear that they have a number of different tools for conducting effects operations. From these sources, it is clear that the British have the ability to conduct a range cyber offensive operations.

---

[24] Ibid., p. 36.
[25] HM Government, 'National Cyber Security Strategy 2016-2021', published 1 November 2016, paragraph 6.5.1, p. 51.
[26] Ibid., paragraph 6.5.2, p. 51.
[27] Edward Snowden Document, GCHQ, 'Full Spectrum Cyber Effects SIGINT as an Enabler for GCHQ's 'Effects' Mission', ca.2010, p. 3, Snowden Surveillance Archive.
[28] Ibid., p. 3.
[29] Ibid. p. 3.
[30] Edward Snowden Document, GCHQ, 'JTRIG Tools and Techniques', Section Effects Capabilities, 05.07.2012, p. 5, Snowden Surveillance Archive.
[31] Ibid., p. 5.

The targets of cyber offensive operations can be seen to be both state and non-state actors. States have admitted that they have considered targeting terrorist organisations via cyber operations, although they do not state how this will take place beyond stopping terrorist use of the Internet.[32] It was also admitted, in February 2016, that US Cyber Command had begun to conduct offensive operations against terrorist organisations such as the Islamic State (IS).[33] In addition, in June 2017, the Defence Secretary Michael Fallon stated that the UK government was at that time 'using offensive cyber routinely in the war against Daesh, not only in Iraq but also in the campaign to liberate Raqqa and other towns on the Euphrates'.[34] Further he argued that these operations are 'beginning to have a major effect on degrading Daesh's capabilities'.[35] It is, however, not just terrorist organisations that have been targeted; hacktivist organisations (A hacktivist group is a non-state actor, such as Anonymous, who use cyber activities for a political purpose) have also been the subject of such activities. There is clear evidence that shows states have also targeted businesses and private companies. From the information that has been shown above, it is clear that the US and the UK governments have both developed a policy of using cyber offensive operations. Although the focus has been on US and UK governments' approach, it is possible, or even likely, that other governments are developing similar policies. It is this author's contention that these operations have a direct relationship with covert action.

Research Aims

This research has a number of arguments. The first argument is that cyber offensive operations are directly related to covert action. This argument will be explained in a number of ways. It will compare the existing understanding of what covert action is to

[32] HM Government, 'The UK Cyber Security Strategy Protecting and promoting the UK in a digital world', November 2011, p. 39.
[33] C.F. the Islamic State has been given a number of different names Islamic State, Islamic State of Iraq and Syria, Islamic State of Iraq and the Levant, and Daesh and others. However, for the purpose of this thesis it will refer to this group as Islamic State (IS). Shane Harris and Nancy A. Youssef, 'U.S. Ratchets Up Cyber Attacks on ISIS', *The Daily Beast*, first published on 18.04.2016, http://www.thedailybeast.com/articles/2016/04/17/u-s-ratchets-up-cyber-attacks-on-isis.html?via=desktop&source=twitter, last accessed on 18.04.2016.
[34] HM Government, Michael Fallon, 'Defence Secretary's speech at Cyber 2017 Chatham House Conference', 27.06.2017, https://www.gov.uk/government/speeches/defence-secretarys-speech-at-cyber-2017-chatham-house-conference, last accessed on 28.06.2017.
[35] Ibid.

cyber offensive operations. When these two are compared this thesis will argue that they are directly related. The second aim of this thesis is to demonstrate how cyber offensive operations are being used to achieve a number of overarching types of activities: propaganda, direct counter propaganda, political, economic and high-end operations. These types of activities will then be compared to the existing understanding of covert action to further allow for a comparison between covert action and cyber offensive operations. By conducting a comparison of the types of activities it will further highlight that there is a direct connection between covert action and cyber offensive operations. This will lead to the argument that overall cyber offensive operations are covert action. However, the thesis will argue against the existing understanding of covert action which merely sees cyber offensive operations as another form of covert action. Finally, this thesis will clearly demonstrate that cyber offensive operations are not new but are continuation of what has already taken place.

There are issues with the research into states use of cyber offensive operations and how they are being used by states. Firstly, at this point in time it is impossible for researchers to know fully and a policy level why states have chosen to conduct these operations. This is because the government documents about particular operations are not available and are still classified. As such, a research can understand that an operation has taken place but not why a government has chosen to use cyber offensive operations to conduct these activities. However, the aim is not to ask why states are using cyber offensive operations but how they are using them and if they should be seen as covert action.

Literature Review

Covert action literature, it could be argued, is missing a great deal on the use of cyber offensive operations. The first mention of the relationship between cyber offensive operations and covert action was by William Daugherty, an academic and a former senior intelligence officer for the Central Intelligence Agency, writing in 2007.[36] He

[36] William Daugherty is an academic and a former senior intelligence officer for the Central Intelligence Agency.

argued that a new form of covert action was beginning to be used.[37] Daugherty labelled this form of covert action as 'information warfare'. Information warfare, was defined as 'either remotely or on-site, a computer, or data banks with the intent of altering or destroying the hardware, software, or information in the computer, is considered to be covert action'.[38] This is now what is more commonly referred to by researchers as cyber war, cyber warfare, or, as this author will argue, should in fact be referred to as, cyber offensive operations. Although Daugherty argued this form of activity had 'enormous potential', he only spends two paragraphs discussing the use of these operations.[39] However, beyond the Daugherty's work, covert action literature has not addressed this issue. This therefore means that the author feels that the use of cyber offensive operations has not been explained by Daugherty. Further, Daugherty argument of information warfare being a form of covert action does not explain the true nature of cyber offensive operations as they are not merely a form of covert action but are being used for all forms of covert action.

It can also be argued that the existing covert action literature fails to take into account the changes in technology that addresses the relationship between covert action and cyber offensive operations effectively. Lowenthal argued in 2009 that there are five main types of covert operations: Paramilitary, Coups, Economic Activity, Political Activity, and Propaganda.[40] Even the Seventh edition of Lowenthal's book, published in 2017 stated that it is likely that cyber offensive operations will be used because it had similarities to other covert action methods. These types of operations were only covered briefly in his work.[41] From this, the thesis will provide a much fuller account of how cyber offensive operations are being used than Lowenthal has achieved.

Another area of disagreement between this author and Lowenthal is that the nature of cyber offensive operations do not easily fit into this theoretical model of covert action. This is because although cyber offensive operations do offer the ability to conduct propaganda operations, political activity, and economic activity, other

[37] William J. Daugherty, 'The Role of Covert Action', in Loch K. Johnson (ed.), *Handbook of Intelligence Studies* (London: Routledge, 2007), p. 283.
[38] Ibid., p. 283.
[39] Ibid., p. 283.
[40] Lowenthal, *Intelligence*, Fourth Edition, p. 169f.
[41] Mark M. Lowenthal, *Intelligence: From Secrets to Policy* Seventh Edition, (Washington, DC: QC Press, 2017), p. 256f.

forms of cyber offensive operations do not fit into the model. To illustrate the argument that cyber offensive operations do not easily fit into the covert action models, it is important to look at an example in the Stuxnet operation. In this operation, the malware specifically targeted the industrial control systems of centrifuges that were creating nuclear material for the Iranians to stop them from working.[42] This example does not fit into the theoretical model of covert action because, it can be argued, it is not economic or political activity, neither is the operation a coup. It does come close to being a paramilitary activity due to the to the damage of actions it may cause yet it is not attempting to overthrow a state using violent means. In Lowenthal's seventh edition, he classes these operations as sabotage. But if the actions were undertaken by an equivalent human force that was supported by an outside power, these would be classed, surely, as a paramilitary operation. This then shows that there is a gap in the existing covert action literature on the types of operations.

These two authors are not alone in failing to acknowledge cyber offensive operations as covert action. This is partly due to the fact that covert action literature was written before the advent of these types of operation or because the aim of the covert action literature is to take a more historical approach to the understanding of covert action.[43]

The existing literature on the use of what this thesis has termed cyber offensive operations can be seen to, firstly, be divided into those sources that provide what could be termed a history of both cyber operations and cyber offensive operations. For example, Fred Kaplan's book *Dark Territory The Secret History of Cyber War* provides a very detailed account of the creation of the US system of using cyber operations and the use of cyber offensive operations.[44] This is similar to the approach of Gordon Corera who in his book *Intercept: The Secret History of Computers and Spies*, illustrates the development and use in both the US and the UK of cyber operations and cyber offensive operations, although he does not use these terms.[45] Similarly, Shane Harris's *@War: The Rise of Cyber Warfare* is another

[42] Thomas Rid, *Cyber War Will Not Take Place* (London: Hurst and Company, 2013), p. 44.
[43] Godson, *Dirty Tricks and Trump Cards*.
[44] Fred Kaplan, *Dark Territory: The Secret History of Cyber War* (London: Simon and Schuster Paperbacks, 2016).
[45] Corera Gordon, *Intercept: The Secret History of Computers and Spies* (London: Weidenfeld and Nicolson, 2015).

example of this form of literature on cyber operations.[46] These sources are very useful in that they examine the development of cyber operations in general and in particular cyber offensive operations. Within this body of literature there are also sources that provide a single case study approach to the study of cyber offensive operations. Kim Zetter's *Countdown to Zero: Stuxnet and the Launch of the World's First Digital Weapon* provides a detailed account of the Stuxnet cyber offensive operation.[47] There is also an extensive body of knowledge about the technical aspects of specific operations. For example, Gaoqi Liang et al.'s article 'The 2015 Ukraine Blackout: Implications for False Data Injection Attacks'.[48] However, some of the sources that focus on a single case of cyber offensive operation tend to fail to theorise what these operations are being used for.

There is also an extensive body of literature that theorises what these operations are being used for. The first real attempt to theorise the use of cyber offensive operations was by John Arquilla and David Ronfeldt in 'Cyberwar is Coming'.[49] This article looks at how cyber offensive operations could be used in the future. In addition, in 2010 Richard A. Clarke and Robert K. Kane published *Cyber War: The Next Threat to National Security and What to Do about it*.[50] Although there are sections of this book that look at actual examples about the use of cyber offensive operations, the book focuses on the speculative nature of cyber offensive operations. This is not always necessarily an issue when it comes to what was then and still is to this day a very novel concept. However, this author disagrees with the way that this book theorises cyber offensive operations. In addition, this author disagrees with the classification of some of the operations it looks at. For example, Clarke classified the cyber offensive operations that targeted Estonia in 2007 as cyber war.[51] Whereas, this author believes that these are, in fact, cyber offensive operations that fall below the threshold of war and should be classified in a different way. From this, there is now

[46] Shane Harris, *@War: The Rise of Cyber Warfare* (London: Headline, 2015).
[47] Kim Zetter, *Countdown to Zero: Stuxnet and the launch of the World's First Digital Weapon* (New York: Broadway Books, 2014).
[48] Gaoqi Liang, Steven R.Weller, Junhua Zhao, Fengji Luo, Yang Dong Zhao, 'The 2015 Ukraine Blackout: Implications for False Data Injection Attacks', *IEEE Transactions on Power Systems*, 32:4, (2017), 3317-18.
[49] John Arquilla and David Ronfeldt, 'Cyberwar is coming!', *Comparative Strategy*, 12:2, (1993), 141-65.
[50] Richard A. Clarke and Robert K. Kane, *Cyber War: The Next Threat to National Security and What to Do about it* (New York: Ecco Paperback, 2012).
[51] Ibid.

an extensive body of literature that seeks to address what cyber offensive operations are and the theory of what they are being used for.[52]

In between these two bodies of literature, there are also sources that address both the historical and theoretical issues of, not only states that are using cyber operations, but also non-state actors who are using cyber operations. One of the best sources for this is P.W. Singer and Friedman Allan's *Cybersecurity and Cyberwar: What Everyone Needs to Know*.[53] In this book, the authors not only deal with the issues that surround states and their use of cyber operations but also non-state actors including terrorism, hacktavist and cyber criminals. This source is especially important as it not only provides examples of cyber operations by looking at specific cases, it also provides a theoretical underpinning for its work. In addition, sources such as Jason Andress and Steve Winterfeld's *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners* take a very similar approach but focus more on the technical aspects of these operations.[54]

This author is not the first to attempt to establish the relationship between covert action and cyber offensive operations. Thomas Rid argued in 2013 that one of the aims of his book *Cyber War Will Not Take Place* was that he 'hopes to take the debate beyond the tired and wasted metaphor of "cyber war"'.[55] His work could arguably be the seminal piece of research on the use of cyber operations. This thesis, therefore, looks to build upon the work of other cyber theorists such as Thomas Rid. However, there are a number of points on which this author will demonstrate some level of disagreement with Rid's book. Firstly, and most importantly, there have been several changes since Rid's book was published. This can be seen in the fact that we have a number of documents that are of critical use to the understanding of these operations. Further, since Rid's book was completed, there have been several cyber offensive operations that have the potential to change the understanding of cyber offensive operations. These include: the operation against *Sony Pictures Entertainment* in 2014; the operations against Ukrainian power stations in 2014-2015 and 2016; and the operations against various elections in 2016-2017, including the US

[52] See Chapter One for a discussion in more detail of these sources and the definitions they provide.
[53] P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford: Oxford University Press, 2014).
[54] Jason Andress and Steve Winterfeld, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*, Second Edition (Waltham: Elsevier, 2014).
[55] Rid, *Cyber War Will Not Take Place*.

presidential election and the French presidential election. Along with these operations, the US and the UK have been conducting cyber offensives against the terrorist organisation IS.[56] These operations are now so important because they have the ability to change the understanding of cyber offensive operations that they need to be looked at in greater detail.

Further, although Rid has come close to following the idea of covert action, he has failed to address what covert action is and why this is so important to the understanding of cyber offensive operations. Although, in part, this author agrees with the characterisation of cyber offensive operations as including sabotage and subversion, there are good grounds on which to challenge his interpretation of the aims of these activities. The main disagreement between this author and Rid is through his work on subversion. In his argument, Rid appears to treat all subversion operations as the same in terms of their violence and the objectives of the operations. However, this author will argue that some of these operations should be seen, in fact, as either political or economic cyber offensive operations (see chapters three and four).

This author also disagrees with some of the ways that Rid classes particular operations. Take for example the cyber offensive operations against one of Saudi Arabia's oil companies, Saudi Aramco in 2012. Rid classes this operation as sabotage.[57] This makes sense in some ways due to the operation being conducted in such a way that it wiped the data from Saudi Aramco's computer. However, this thesis will argue that instead of looking at how the operation was conducted, it is more important to understand what the operation aimed to achieve. In chapter three, this thesis will demonstrate that this operation should be seen as a political cyber offensive operation rather than cyber sabotage due to nature of the operation and its apparent aims. Further, this author disagrees with Rid's interpretation of Disturbed Denial of Service (DDoS) that he classifies as being sabotage. DDoS attack is where many connected devices are used to request access to a website causing the website to crash. However, this author would argue that this is much more akin, using Rid's phrasing, to a 'subversion operation'. This is because although there is some level of sabotage to the operation, the operation is much more concerned with achieving a

[56] These operations will be looked at in detail in chapters 3 and 4 below.
[57] Rid, *Cyber War Will Not Take Place*, p. 55.

political objective, thus making it a subversion or, in this author's opinion, a political cyber offensive operation that is looking to stop a government website from working. Finally, Rid has focused on showing the ways that both state and non-state actors have conducted cyber operations and appears to treat these as all being the same. The purpose of this thesis is to focus on the ways that states have and can use cyber offensive operations. The reason for this is that there may be differences in how states conduct their operation to those conducted by non-state actors.

In addition to Rid's work, this thesis will also build upon the work of Aaron Brantly who in 2014 further addressed the relationship between covert action and cyber offensive operations.[58] Brantly addressed two cyber offensive operations: the Stuxnet operations and the Israeli operation to stop Syrian Air Defence network from functioning.[59] This is similar to Lowenthal's work on covert action and sabotage. However, this author will demonstrate that cyber offensive operations are being used to conduct more than this form of covert action. In addition, as was the case with Rid's work, there is now a need to update Brantly's work to fully understand covert action.

Due to the fact that, as was shown above, the covert action literature does not investigate the use of cyber offensive operations and both the US and the UK governments have expressed through their policies an attempt to use cyber offensive operations, there is a need to undertake this research.

Methodology and Sources

Due to the fact that this is a subject that keeps evolving, the author will not assess any new case or information about cyber offensive operations from 31 of July 2017. The reason that this date was chosen was because it can take a long period of time for information and confirmation on cyber offensive operations to enter the public domain.

The thesis will compare the use of cyber offensive operations to understanding of covert action, using a comparative case study methodology. It was argued by

[58] Aaron F. Brantly, 'Cyber Actions by State Actors: Motivation and Utility', *International Journal of Intelligence and CounterIntelligence*, 27:3, (2014), 465–484.
[59] Ibid., 477-480.

Charles Ragin that 'comparison provides a basis for making statements about empirical regularities and for evaluating and interpreting cases relative to a substantive and theoretical criterion'.[60] What covert action is and the activities that come under this umbrella are already well established within intelligence studies. From this, it will use the comparison methodology to address what cyber offensive operations are being used for and how this affects the interpretation of these operations.

To allow for the comparative approach, the author has chosen the methodological approach of case studies. This was chosen as, it was argued by Eisenhardt, this methodology permits a cross-case patterning to allow for a theory to develop.[61] The case study approach is a mixture of what is termed an idiographic theory guided case study approach and the plausibility probe case study approach. The idiographic theory guided the research 'in that they aim to explain and/or interpret a single historical episode rather than to generalize beyond the data'.[62] In addition, the aim of a plausibility probe is to 'give the reader a "feel" for a theoretical argument by providing a concrete example of its application, or to demonstrate the empirical relevance of a theoretical proposition by identifying at least one relevant case'.[63] The approach to the case studies is extensive rather than intensive. This is because it will allow the author to collect as many instances of cyber offensive operations that have been used rather than focusing on a smaller number of operations and examining these in depth. It will not be looking into any one case in great detail but using all of the cases of cyber offensive operations that can be discovered to interpret these events within a well acknowledged theory in intelligence studies. It was argued by Harry Eckstein, in a comparison between comparative and case study theories, that there are six options for using the two together to build up a theory. From the options of case study and comparative studies that were offered by Eckstein, option three has been chosen. This is where case studies should be conducted for the

[60] Charles C. Ragin, *The Comparative Method: Moving Beyond Qualitative and Quantitative Strategies* (Berkeley: The University of California Press, 1989), p. 1.
[61] Kathleen M. Eisenhardt, 'Building Theories from Case Study Research', *The Academy of Management Review*, 14:4, (1989), 532-550, 533.
[62] Jack S. Levy, 'Case Studies: Types, Designs, and Logics of Inference', *Conflict Management and Peace Science*, 25:1, (2008), 1-18, 4.
[63] Ibid., 25:1, 1-18, 6.

purpose of discovering theory.[64] It was argued by Eckstein that the use of the option is that it allows for a theory building case study approach to be conducted. He argued that 'if a subjects and insights for comparative studies are wanted, case studies can provide them' using this option.[65] Further, the evidence that has been gained from these case studies will be used to construct a generalised theory. A generalisation approach allows a researcher to compare several cases together.[66]

The case study approach and the generalisation approach will be combined with the research methodology of historians. It was argued by Mark Philp that the craft of a historian is to use historical data to understand a feature of the contemporary world.[67] In addition, this thesis uses history to inform political theory. Further, Philp argued that political science might look to history to understand events.[68] This is because it will look at past instances of covert action, and past instances of cyber offensive operations to clearly understand how these two connect. It is clear then that this thesis is using a broad approach using both historical and political science methods to understand the existence of cyber offensive operations and what this means to our understanding of their use. By using this comparative approach it allows the author to achieve the objective, of allowing this author to compare historical information to the contemporary world.

When it comes to the use of sources in studying intelligence it was argue that 'government secrecy is a major problem for anyone doing any branch of political studies in the United Kingdom'.[69] This statement may have even greater meaning when studying contemporary intelligence and security issues. Although, with the growth of the Internet, and some states following a policy of transparency with intelligence and security related issues, the actual ability to gather official primary source material can be difficult. When conducting a historical study of intelligence, historians need to assess historical primary sources. This can be seen in the fact that

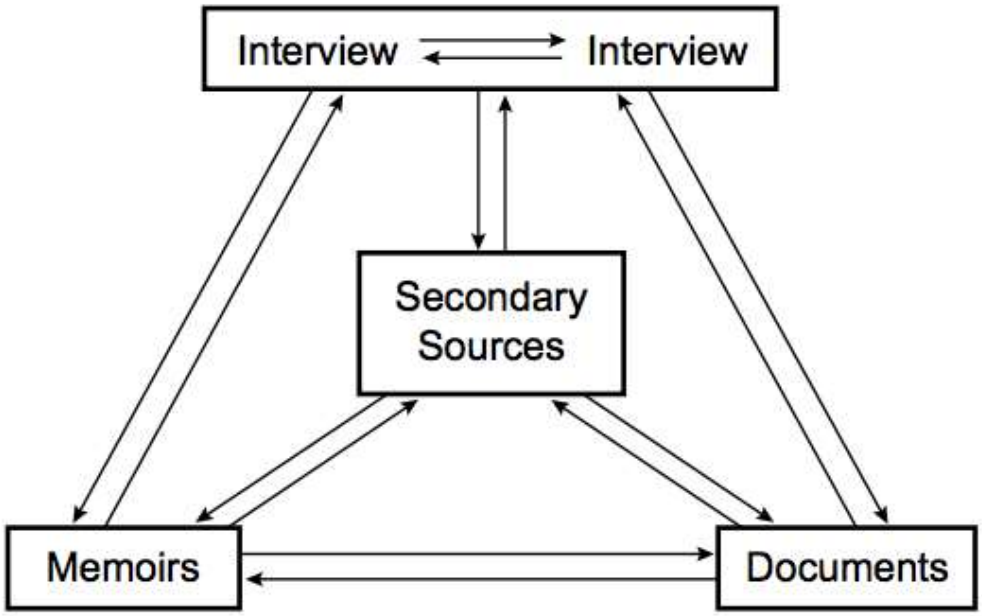
[64] Harry Eckstein, 'Case Study and Theory in Political Science', in Roger Gomm, Martyn Hammersley, and Peter Foster (eds), *Case Study Method: Key Issues, Key Texts* (London: SAGE Publications, 2000), p. 129.
[65] Ibid., p. 129.
[66] Uwe Flick, *Introducing Research Methodology A Beginner's Guide to doing A Research Project* (London: SAGE Publications, 2nd edn, 2015), p. 122.
[67] Mark Philp, 'Political Theory and History', in Marc Stears and David Leopold (eds), *Political Theory: Methods and Approaches* (Oxford: Oxford University Press, 2008), p. 129.
[68] Ibid., p. 129.
[69] Philip H.J. Davies, 'Spies as Informants: Triangulation and the Interpretation of Elite Interview Data in the Study of the Intelligence and Security Services', *Politics*, 21:1, (2001), 73-80, 76.

intelligence and security documents that were archived have been released into the public domain. This had led some to argue that in the 1990s the US and the UK had developed a greater openness towards security and intelligence related matters.[70] This began in the UK with the Waldegrave initiative 1993, although, this has issues, as was shown by Richard Aldrich,[71] and has recently been supported with the introduction UK Freedom of Information Act 2000. The use of the FOIA to study intelligence and security, as demonstrated by Christopher Murphy and Daniel Lomas, has allowed academics to access to additional documents.[72] Despite the difficulties gaining access, these systems benefit the study of historical intelligence and security related issues.

To study contemporary issues of intelligence and security, there is a need to look at other ways of gathering information. Davies argued that academics that are interested in studying intelligence and national security should conduct a research methodology in which they use three different forms of primary sources and compare them to increase their understanding of the issue.[73] The three sources that Davies looked at were interviews, memoirs, documents, and, in the middle, secondary sources. Triangulation aims to provide a cross-reference between sources.

[70] Richard Aldrich, ‘‘Grow Your Own’: Cold War Intelligence and History Supermarkets’, *Intelligence and National Security*, 17:1, (2002), 135-152.
[71] Ibid., pp. 135-52.
[72] Christopher J. Murphy and Daniel W. B. Lomas, ‘Return to Neverland? Freedom of Information and the History of British Intelligence’, *The Historical Journal*, 57:1, (2014), 273-87.
[73] Davies, ‘Spies as Informants’, *Politics*, 76.

Figure 1: Triangulation of Sources.[74]



The idea is that by using these sources together an intelligence scholar will be able to build up a clearer understanding of intelligence. Yet this author would argue that, when studying intelligence and security related issues that are not historical and that took place in the twenty first century, there is a need to update this to reflect the new information that is available. These sources now include: interviews, news sources, official documents, archived documents, leaked documents and cyber security companies' reports. Although Davies' triangulation theory does not exclude the use of non-official documents such as leaked documents and private security documents, the author wishes to highlight these as sources. The author believes that the triangulation model offered by Davies still works, it is just that the new sources need to be addressed. The next part of the Introduction will outline all of the categories of sources that will be used within this thesis (interviews, news articles, official primary documents, leaked documents, and, cyber security reports) and the issues with these sources. When research follows the policy of triangulation, it is possible to alleviate some of these issues.

Interviews

Davies argued that 'Elite interviewing is a central tool in the study of intelligence and security services, not least because intelligence is something created by, of and for the

[74] Ibid., 76.

policy-forming and decision-making elites in national government'.[75] Although this author would have liked to have conducted interviews with members of US and UK governmental departments that deal with the use of cyber offensive operations, this was not possible. This author contacted the Intelligence and Security Committee in the UK to ask for an interview. The Committee's secretary informed the author that due to the nature of the issue and the national security implications this would not be possible. The present study is about more modern phenomena, which has it meant that there could be much more secrecy to the types of operations than was the case with the topics Davies discussed. In addition, identifying former members of intelligence services around the issue of cyber is difficult because it is a relatively new phenomenon and is shrouded in secrecy.

There is, however, a way round this to allow intelligence and security scholars to still use elite interviews. Elite interviews are classed as interviews with those in a position of authority within a government or organisation and who know about a particular policy, operation, or procedure. This author has made use of interviews that have been conducted by others but that are publicly available along with other governmental hearings. This is not to say that there were not any issues with using this methodology to conduct research. Firstly, and most importantly, the researcher is not guiding the questions. This means that a researcher is forced to rely on others to ask the questions. This was, however, not an issue that this research has found to be of great concern. Most of the interviews provided the evidence needed. In addition, there was a benefit to using this research method in that there was, at times, new information that came out in these interviews. This was because, with others asking the questions, they came up with different approaches to questions that at first seemed irrelevant for the thesis but the answers provided invaluable information. Further, the interviews, especially those conducted during various Aspen Security Forums conferences, used interviewers who were widely known. This meant that they may be an extra layer of trust, or at the very least, recognition between the interviewer and the interviewees. This may have allowed for far more detailed responses than the author may have been able to get from the interviewees.

In addition to interviews that have been conducted by others, this author has made use of hearings conducted in the US about the work of intelligence. The Senate

[75] Ibid., 76.

and House hearings have proved to be some of the most enlightening forms of information that this author has been able to access for this study. These hearings were conducted by members of Congress that oversee the work of both intelligence and military organisations. The focus of these hearings has been the role of the NSA and US Cyber Command and their use of cyber offensive operations. Further, with Russia's involvement in cyber offensive operations against the US presidential elections in 2016, there is a large volume of information in these hearings that is available to the author. Although these hearings were unclassified and, as such, the attendants of the hearing will only answer questions that are unclassified, the author would still have, if he had conducted the interviews himself, only received unclassified information. In addition, these hearing have a further benefit, if this author had been able to conduct interviews, it would have been unlikely, if not impossible, that he would have been able to have had interviews with senior members of the intelligence and armed forces community. Whereas, these hearings are conducted by members of Congress who have the legal authority to have these high members of the US intelligence and armed forces community to testify before them.

Newspaper Articles

As this thesis will focus on contemporary issues, this author has made use of news articles to support other source material. There is a long tradition of media and news accounts being used in the study of intelligence and security. When intelligence and security services have been seen to have conducted activities that are deemed to illegal or immoral, it is often through the media that the general public and the wider research community discover these issues. It has been argued that it can often be that the media plays a role in providing oversight of intelligence agencies. If the media investigates a troubling area of what the intelligence services are doing and discovers and publishes a story, this shocks other oversight bodies into addressing and investigating these issues.[76] Claudia Hillebrand stated that some of the notable cases of the media discovering issues and publishing them are the abuse of Abu Ghraib and US rendition of terrorist suspects.[77] In addition, it has been noted by Christopher Moran that intelligence accounts that have been produced by journalists have been

[76] Loch K. Johnson, 'A Shock Theory of Congressional Accountability for Intelligence', in Loch K. Johnson (ed), *The Handbook of Intelligence Studies* (London: Routledge, 2007), p. 345.
[77] Claudia Hillebrand, 'The Role of News Media in Intelligence Oversight', *Intelligence and National Security*, 27:5, (2012), 689-706, 690-91.

very good at finding out information which intelligence authorities have wanted to keep secret. For example, in 1946 Stanley Firmin produced a book that included details of British intelligence deciphering German codes.[78] News accounts have always been important sources for understanding and investigating intelligence agencies. The present study will focus on newspaper articles from news organisations that have gained a reputation as being trustworthy. These include *The New York Times*, *The Washington Post*, *The Daily Telegraph*, *The Independent*, *The Guardian*, and *BBC News*.

It is often claimed that 'journalism is the first draft of history', implying that the information contained within it will not always be correct.[79] This might mean that researchers may not use information from news articles. Much of this is based on the idea that news articles do not have the same ability to look for all the facts, as they must provide the information in a timely fashion. However, it must be noted that news articles are not the only source from which information may be missing. It must be pointed out that many historians writing about the history of the Second World War before the secrets of Bletchley Park had become known had to be re-written because information was missing not from newspaper articles but from historical documents.[80]

News articles have the ability to provide information that other sources lack. One reason is that journalists have the ability to cultivate sources over a long period of time. It was argued, in relation to a book written by a journalist, that because the author had privileged access to sources, he was able to provide a better account of these operations than others would have been able to. This was because the author was able to have access to sources that others would not be able to access.[81] News articles will be used to provide factual information about an operation or the existence of the operation. The interpretation of these operations and what they tell the world about these operations will be produced by the author.

However, one problem that is faced by academics when using news articles as sources is that there have been times in the past when governments have provided

[78] Christopher Moran, 'Intelligence and the Media: The Press, Government Secrecy and the 'Buster' Crabb Affair', *Intelligence and National Security*, 26:5, (2011), 676-700, 681.
[79] This is a cliché term that has been linked to a number of people.
[80] Christopher Andrew, 'Intelligence, International Relations and 'Under-theorisation'', *Intelligence and National Security*, 19:2, (2004), 170-184, 174f.
[81] Ross D. King, 'Intercept: The Secret History of Computers and Spies', *Intelligence and National Security*, 32:6, (2017), 875-78, 876.

information to journalists that is intentionally and knowingly false so that journalists will then spread this information.[82] Nevertheless, this would always be a problem no matter if someone interviewed a person on their own, or was given information from news articles. This is to note that the author is aware of this issue. This does not mean that there will not be problems with the information that has been provided to the journalist. One problem is that the information that is contained in the article will, at times, be quoted from anonymous sources or give a reference to a position rather than a named person. For example, some articles have a statement similar to 'a source close to the president' or an unnamed source high up in the administration or a particular organisation. The danger of this is, as was argued by former Federal Bureau of Investigation (FBI) Director Jim Comey, is that when a news article talks about a classified source

> it doesn't come from the people who actually know the secrets. It comes from one hop out, people who heard about it or were told about it. And that's the reason so much information that reports to be accurate classified information is actually wrong in the media.[83]

Nevertheless, it could be argued that although it will never be resolved completely, this will be mitigated by using news reports that have come from a newspaper that has achieved a good reputation. This means that there must be a level of trust placed on the researcher that the journalist has checked in some way that the person that they are quoting would have access to the information.

Official Primary Documents: Contemporary and Archived

The study will also use contemporary official primary source documents that have been released by governments into the public domain. An example of these types of documents includes documents released by the Department of Defense in 2015 and the Intelligence and Security Committee's reports. However, it must be noted that there are a number of issues with these sources. To begin with, some of the sources are highly redacted. Further, as the documents that are covered here are publicly available, it means that the information that has been contained within these sources

[82] This is not simply paranoia as during the Second World War, the British government placed information in newspapers that was intended to spread the information. Furthermore, Chapman Pincher, a reporter for the *Sunday Express* admitted that he was used to spread false information. See Chapman Pincher, 'A Lifetime of Reporting on Intelligence Affairs', in Robert Dover and Robert Goodman (eds), *Spinning Intelligence: Why Intelligence Needs the Media, Why the Media Needs Intelligence* (London: Hurst and Company, 2009), p. 155.

[83] Jim Comey, House Permanent Select Committee on Intelligence, 'Hearing On Russian Active Measures Investigation', *Political Transcript Wire*, 20.03.2017, Transcript, p. 39.

has been deemed unclassified or declassified. This means that there will always be an amount of information, most likely a large amount, due to the subject matter, that will not be released. This does not mean that the information contained within them will not be of use. This is because, at times, information can be inferred from what is contained allowing a researcher to take an educated guess at what information is not there even if they do not know with certainty.

Another form of sources that this project is using is archival documents. These will be used extensively in the second chapter of the thesis. They allow the present study to look at historical examples of covert action to see if there are parallels between covert action and cyber offensive operations by allowing for an understanding of the use of covert action and the forms of activity that are classed as covert action. There are a number of problems relating to the use of archival documents in the study of intelligence related subjects. Although much of the danger of using archival sources for the study of intelligence and intelligence related issues has been covered elsewhere, it is important to note that the researcher is aware that historical documents may not provide the complete picture.

Leaks

The most controversial source of information that will be used for this thesis is leaked documents. The documents that will be of most use are those released by Edward Snowden who, in 2013, began to leak documents that he had illegally taken from the NSA. It has been alleged that Snowden took around 1.5 million documents.[84] The thesis will also use those documents that have been leaked to *Wikileaks*. Although most of the points that will be made from this here will relate more directly to the use of the documents leaked by Edward Snowden, the methodological issue with using documents not only apply to using the files from *Wikileaks*, but also to the use of leaked documents for research generally.

The use of such documents poses questions for researchers. Firstly, and most importantly, is the issue of accuracy. This is a problematic area. It has been pointed out that no one in the general public knows the accuracy of the information that these sources contain. Intelligence services have been keen to never confirm or deny that these documents were genuine, or if any of the information was correct. In addition,

[84] House Permanent Select Committee on Intelligence, 'Review of the Unauthorized Disclosures of Former National Security Agency Contractor Edward Snowden', published, 15.09.2016.

the allegation that the NSA was spying on the German Chancellor Angela Merkel that first came to into the public attention in 2013, has failed the criminal level of proof. This is because when the information that was contained within the Edward Snowden documents about the alleged spying on Chancellor Merkel's phone came to court, the court stated that the information did not provide the sort of proof that was needed to allow the case to carry on.[85] However, it must be pointed out that others believe that this case was stopped for a political motivation rather than any evidentiary issues with the documents and the information contained within them.[86] Whether the case was stopped because of lack of evidence, or because there was political pressure is unlikely to be made public for a long time, if at all. Yet it should also be noted that criminal cases have a burden of proof attached to them. This means the evidence has to be shown to be correct, which these leaked documents as a standard could not meet. This means that in this case the question of accuracy is set to last. However, it is also worth noting that not all investigations have believed that the information is false. The Senate Select Committee on Intelligence used the information in a number of enquiries, although they have also had access to information that goes beyond the documents.[87] From this then it could be argued that perhaps the information that is contained within the documents has some level of accuracy.

Nevertheless, there is also no way to know whether all the documents are genuine. It is not impossible to believe that someone either within the intelligence community, Edward Snowden himself, or someone related to the release of the documents could have changed the information within them. There is evidence to show that there have been times in which people have tried to place fake documents into the public domain. This can notably be seen in the fact that in 2017 an unidentified person tried to pass off fake documents to a news agency that they alleged were leaked. This document turned out to be false.[88] This then shows the danger of using leaked documents to conduct research as the documents could be fake. However, it can also be seen that, as has been pointed out above, official

[85] Ewen MacAskill, 'Germany drops inquiry into claims NSA tapped Angela Merkel's phone', *The Guardian*, first published 12.06.2015, accessed via Nexus Business and News.
[86] Ibid.
[87] Senate Select Committee on Intelligence, 'Open Hearing: FISA Legislation', 26.09.2013.
[88] The Rachel Maddow Show, 'Maddow to news orgs: beware of forged Trump Russia documents!', first published 06.07.2017, http://www.msnbc.com/rachel-maddow/watch/maddow-to-news-orgs-heads-up-for-hoaxes-985491523709, last accessed on 06.07.2017.

organisations have accepted, at least in part, some of the information into their enquiries and, as such, the information probably has a basis in fact.

Furthermore, although there is no evidence to state that the information is true, there has equally not been any information that as of yet that indicates the information is, in fact, false. For example, The House Permanent Select Committee on Intelligence report into Edward Snowden did not indicate that any of the documents were faked.[89] This means that an academic would be remiss if they failed to use the information that is contained within it. In these ways, it could be argued that the evidence based reason for not using the information does not support not including the information.

There is a further problem with using the information that has been contained within the leaked documents. The documents are fragmented. Take for example a document that will be used heavily in the third and fourth chapters: 'JTRIG Tools and Techniques'. The document states a code name for a tool that has been developed by this section of GCHQ, and a rough idea about its ability.[90] There is no further information contained. An academic would be remiss not to use this information, yet due to its fragmented nature, there is a danger that a researcher may misidentify or misinterpret a particular point due to the fragmentation of the documents. This leads to the point that the information contained within these documents may in fact not be false, but they may be missing so much information that they become misleading. However, it must also be noted that this is not the only type of source with this issue. It is clear that documents are missing in a number of cases in the study of history and it is an academic's job to piece information together.

The final issue is whether the documents should be used at all because of the danger of publicising information that may damage national security or endanger lives. This is not simply related to using the information that has been contained within the Edward Snowden documents but much more generally to using leaked documents. The main issue of using leaked documents, even the Edward Snowden files, is that the person who is discussing them is drawing attention to them. It is possible that some of the information contained within these documents were missed

[89] House Permanent Select Committee on Intelligence, 'Review of the Unauthorized Disclosures of Former National Security Agency Contractor Edward Snowden', published 15.09.2016.
[90] Edward Snowden Document, GCHQ, 'JTRIG Tools and Techniques', 05.07.2012, Snowden Surveillance Archive.

by states or terrorist groups, and that by discussing these documents, a researcher is highlighting an issue that might been missed or even, the researcher may in fact clarify an issue that these states or groups missed. Furthermore, there could be a damage caused by highlighting an issue within a document. It has been claimed that, especially around the Edward Snowden documents, the information that has been contained within them has helped 'the enemy'. The House Permanent Select Committee on Intelligence has just under four pages dedicated to examples of Snowden documents that had 'caused massive damage to national security' although these are all redacted.[91] However some claims have been made public. For example, it was claimed by the former director of the CIA John Brennan that 'a number of unauthorised disclosures' as well as new laws enacted in the US, had helped the IS terror groups in their attacks in Paris in 2015.[92] However, in 1996 it was reported by *The Washington Post* that Al Qaeda had already stopped using mobile phones due to fears of intelligence agencies being able to intercept these communications.[93] However, there have been other claims about Edward Snowden helping the enemy. For example, it has been argued that because of the information that was contained within the documents the British foreign intelligence service, Secret Intelligence Service (SIS), were forced to remove agents that were in Russia.[94]

Although there has been no proof of these events having been directly caused by these leaked documents, if it was true, it shows that there are dangers in using leaked documents for information. Nevertheless, in terms of this thesis and academics using leaked documents, it is clear that there is a danger of highlighting information that has been either missed as was noted above. However, it must also be stated that in terms of the leaked documents that are being used here, the danger of adding publicity does seem a little redundant. This is because the documents themselves have

[91] House Permanent Select Committee on Intelligence, 'Review of the Unauthorized Disclosures of Former National Security Agency Contractor Edward Snowden', published 15.09.2016, pp. 24-28.
[92] David Smith and Dan Roberts, 'CIA Chief Criticises recent Surveillance Rollbacks in wake of Paris Attacks', *The Guardian*, first published, 16.11.2015, https://www.theguardian.com/world/2015/nov/16/cia-director-john-brennan-criticises-surveillance-reform-paris-attacks, last accessed on 16.11.2015.
[93] Glenn Kessler, 'File the Bin Laden Phone Leak Under 'Urban Myths', *The Washington Post*, first published, 22.12.2005.
[94] Nicola Harley, 'British spies removed from operations after Russia and China crack codes to leaked Snowden files' *The Daily Telegraph*, first published 14.06.2015, http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/11673533/British-spies-removed-from-operations-after-Russia-and-China-crack-codes-to-leaked-Snowden-files.html, last accessed on 15.06.2015.

received so much media attention that it is hard to believe that anyone would gain in the extra knowledge from these documents that will be used in this project.

Cyber Security Reports

When studying the use and the effectiveness of cyber offensive operations, academics also benefit from Cyber Security reports written by private companies, including *McAfee*, *Symantec*, and *Kaspersky Labs*. This is because these organisations spend most of their time researching cyber security issues, they have the infrastructure to conduct investigations of attacks, and they can take their time investigating an issue before releasing a report. They also have a business reputation to maintain. This means they are unlikely to publish information that is untrue. However, a note of caution must also be applied to these sources. Their business is cyber security. They make money from the fact that criminals and states are using the cyber world to attack people as they sell produces that are designed to stop these attacks. This means that there is a possible vested interest in making an attack seem more likely or even increasing the danger of an attack.

In these ways, it is clear that when investigating intelligence and security for contemporary issues, there are a lot of sources that researchers have to allow them to investigate the issues. Yet there is still a need for researchers to follow the idea of conducting triangulation. As each source has potential issues the researcher must combine these sources together. They must also compare these sources to allow them to understand the issues and present as clear a picture as possible.

Structure of the thesis

To address the overall aim of the project that is to understand the relationship between cyber offensive operations and covert action, this thesis will be divided into six chapters.

The first chapter will establish and justify the focus of cyber offensive operations and covert action together. To do this the author will demonstrate why he has rejected the term cyber war to describe cyber offensive operations. It will argue that cyber war is not what people are discussing when they use the term for an event; as such, cyber war is a misnomer. This chapter will provide a brief definition for what

war is. This chapter will then critically assess the definitions that have been offered by others when they refer to cyber war. It will argue that the definitions of cyber war do not work when they are examined in depth. It will take a thematic approach at studying the theories that others have put forward about the nature of cyber war and will argue that their attempts to define cyber war have failed. Finally, this chapter will provide a definition of cyber war based on what war is. It will, however, also argue that a cyber war, based on this definition, is unlikely if not impossible. This is because it will argue that for a cyber war to happen it must be contained within the cyber world, but also have a level of threat that is equivalent to war. This chapter will show that instead of the incidents of cyber offensive actions being called cyber war, they must in fact be labelled another way. The chapter will then establish the understanding of covert action. To begin with, it will address what precisely covert action is. The final part of this chapter will clearly demonstrate that in terms of how the activities have been envisaged, a direct connection between cyber offensive operations and covert action.

The next three chapters of this thesis will support and further demonstrate the connection between covert action and cyber offensive operations. This chapter will seek to compare and contrast these various theories and highlight the main areas of what constitutes covert operations in theory. It will argue that there are four overarching ways that covert actions have been used: propaganda, political, economic, and paramilitary. These chapters will examine the overarching ways that covert action has been used to operations that can be seen to have, or likely could, take place using cyber offensive operations. This thesis will demonstrate that there are six overarching ways that states can use cyber offensive operations to target other states as well as non-state actors. It will argue that cyber offensive operations can be seen to follow a hierarchy of violence due to what the operation is trying to achieve. The six overarching ways that it will argue that cyber offensive operations can be used are: propaganda, direct counter propaganda, political operations, economic operations, and high-end operations. It will also argue that these are the ways in which the US and the UK can use cyber offensive operations in the future. Each of these chapters will compare these types of operations to the traditional understanding of the forms of covert action. They will clearly demonstrate that in terms of the forms of activities cyber offensive operations and covert action can be directly compared to

each other and that overall there is nothing new happening with states use of cyber offensive operation than to that of covert action.

The fifth chapter of the thesis will compare and contrast the second chapter of the thesis that looked at covert action theory with that of the examples of the use of cyber against state and non-state actors. The purpose of this chapter is to highlight that cyber offensive operations are a means of conducting covert action. It will also demonstrate the flaws of the existing sources on covert action that include cyber offensive operations. This means that the chapter will develop a new theoretical model of covert action that includes the use of covert action achieved through cyber means. This chapter will also argue that the fact that covert action is being achieved through cyber means presents a number of intelligence organisational challenges as there are now many different competing organisations that could, in theory, claim some level of control of covert action via cyber means, including traditional covert action agencies like the CIA in the US, SIS in the UK and even the military. It will demonstrate the dangers of having many different agencies all having a role in covert action. This will be achieved by illustrating with historical examples how having a number of organisations that had a role in covert action created the issues that some states faced.

The final chapter of the thesis will address the ethical issues of using covert action, both in its traditional form (the activities identified in chapter two), and covert action through cyber means. This is to understand if there are any new ethical issues around the use of covert action achieved through cyber means. It will argue that although there are no substantial changes to the ethics of traditional covert action compared to covert action achieved through cyber means, there are a number of points that states need to be aware of if they are to conduct these types of activities ethically. The ethics of these operations will be grounded within Just War Theory. This chapter is needed because much of the ethics of cyber offensive operations has been focused on the fact that they are war rather than covert action. This means that intelligence and government agencies, as well as academics, need to adapt the debates around the ethics of these operations towards a covert action framework rather than cyber war or cyber warfare.

CHAPTER ONE

Cyber Offensive Operations and Covert Action

This chapter will clearly demonstrate that cyber offensive operations are covert action. To achieve this, the chapter will firstly have to demonstrate that cyber offensive operations are not, and should not, be termed cyber war. It will do this by firstly providing a concise summary of what war is. It will argue that for something to be termed war it must firstly, it must be political in nature, secondly, it must have a level of violence, although it is not debated whether all wars will have an element of chance or as Clausewitz refers to it at different points, and there has to be a substantial level of threat for something to be war. If something that has been termed war does not have these elements, then it is not war. Using this definition of war it will then compare how other academics have defined cyber war. It will however argue that overall these definitions of cyber war do not work. To illustrate this point this chapter will provide a definition that this author would actually fulfil the definition of cyber war. It will then demonstrate why this definition would not work.

This chapter will then demonstrate and evaluate what covert action is and the forms of activities that are usually seen as covert action. It will do this, firstly, by looking at the definition of covert action to show what covert action is but, also, what it is not. It will demonstrate that covert action is usually used by one state against another state. It will, however, also argue that covert action has, at times, included operations against terrorist organisations. This will be illustrated by showing that some of the methods of covert action have been used against terrorist organisations. As such the notion of what covert action is should also include that covert action can target non-state actors such as terrorist organisations. It will follow the approach of Loch Johnson, William Daugherty, Mark Lowenthal, and others who explain the type of operation and provide a brief historical outline to the operations.

The final section of this chapter will clearly demonstrate that cyber offensive operations are covert action. This part of the chapter will clearly argue that cyber offensive operations are covert action based on the fact that they are aimed at

changing a behaviour of an adversary, they maintain a level of plausible deniability, and they are in fact covert action.

Cyber Offensive Operations are not Cyber War.

Cyber war is a contentious term. It has been noted that the term cyber war or cyber warfare has become 'so ill defined in discussions that it can … be stated that the terms have lost all meaning'.[1] Part of the problem is that there are those who use the term cyber war or cyber warfare but do not define what is meant by these terms. An example of is Chris Grey, who makes the claim that cyber war exists but does not actually define it.[2] However, what must be noted about this claim is that it was published in 1997. From that, it could be argued that the actual threat of cyber offensive operations was lower than it has now become and it was a new phenomenon. A possible explanation for the lack of definitions include that, as a term, it is difficult to define and appears to be something equivalent to a 'you know it when you see it' type event. Due to the fact that cyber war is a contentious term, it is worth assessing the definitions of that other authors have offered to attempt to understand what a cyber war means.

It can be seen that what war actually is has a very particular meaning. However, it can be argued that the best traditional theorist of war and war's relation with politics was Clausewitz. All the way through *On War,* it is clear that Clausewitz felt that politics and war were directly connected. Clausewitz noted that 'war is simply a continuation of political intercourse, with the addition of other means'.[3] Clausewitz went on to argue that 'the political object is the goal, war is the means of reaching it, and means can never be considered in isolation from their purpose'.[4] 'Thus policy converts the overwhelmingly destructive element of war into a mere instrument'.[5] Finally, 'only if war is looked at in this way does it reappear; only then

[1] Misha Glenny and Camino Kavanagh, '800 Titles but No Policy—Thoughts on Cyber Warfare, American Foreign Policy Interests' *The Journal of the National Committee on American Foreign Policy*, 34:6, (2012), 287-294, 289; This argument was supported by Liff who argued, 'the meaning of 'cyberwarfare' has become so convoluted in popular discourse' see Adam P. Liff, ''Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War', *Journal of Strategic Studies*, 35:3, (2012), 401-428, 404.
[2] Chris Hables Grey, *Postmodern War: The New Politics of Conflict* (London: Routledge, 1997), see the first chapter, but especially pp. 23-25.
[3] Carl von Clausewitz, *On War*, Michael Howard and Peter Paret edited and translated (Princeton: Princeton University Press, 1976), p. 605.
[4] Ibid., p. 87.
[5] Ibid., p. 606.

can we see that all wars are things of the same nature; and this alone will provide the right criteria.'[6] Although these are not the only places that Clausewitz stated the relationship between politics and war, all of these quotes serve to demonstrate that for Clausewitz, one of the most important elements of war is the fact that there must be a political objective behind it. Clausewitz was not the only theorist of war to believe that war must have a political element to it.[7] From this, it can be seen that most of the traditionalists feel that there must be a political motivation behind the fighting for it to be war.

In addition to this, the political objective of war is the motive for the action.[8] Clausewitz further argued that 'war is a clash between major interests which is resolved by bloodshed'.[9] From all of these quotes, it has not been stated that 'policy' is directly related to the state. Peter Paret, noted that, for Clausewitz, war is an expression of all forms of political life which have been shaped by a number of qualities. From this, war is an act of force undertaken to bring about change.[10] Again this change can be related to non-state actors as well as states. To support this, Smith argued that, if policy and politics in violence were only being related to the state and government that would mean the exclusion of groups like the Irish Republican Army (IRA) who were not a state but deemed themselves to be.[11] In this way, it is clear that the IRA did have a politically motivated reason for conducting their campaign.

The aim of war is to make the enemy fulfil a particular will, from this the will is reason for war and as such the policy behind the war.[12] Jan Honing argued that Clausewitz can explain intra-state wars because 'any form of warring organisation that do not form states … any community has its leaders, fighters, and common people'.[13] It is clear that even in the context of intra-state conflicts the political

[6] Ibid., p. 606.
[7] C.F. To support this see for example; Antoine Henri Jomini, *The Art of War*, Edited and Translated Brig Gen. J.D. Hittle (New Delhi: Natraj Publishers, 2005), p. 45; Niccolo Machiavelli, *The Art of War*, translated by Henry Neville (New York: Dover Publications, 2006), p. 8; Mao Tse-Tung, *The Art of War* (Texas: El Paso Norte Press, 2005), p. 5; Sun Tzu, *The Art of War*, James Clavell (ed) (London: Hodder and Stoughton, 1981), p. 23.
[8] Clausewitz, *On War*, p. 80.
[9] Idid., p. 149.
[10] Peter Paret, 'Clausewitz' in Peter Paret (ed), *Makers of Modern Strategy: From Machiavelli to the Nuclear Age* (Princeton: Princeton University, 1986), p. 202.
[11] MLR Smith, 'Strategy in an age of Low-Intensity Warfare: Why Clausewitz is still more Relevant than his Critics', in Isabelle Duyvesteyn and Jan Angstrom (eds), *Rethinking the Nature of War* (London: Frank Cass, 2005).
[12] Ibid., p. 35.
[13] Ibid., p. 49.

element is there and can be explained by Clausewitz's view of war. In all of these ways, it is clear that although critics have claimed that there might be occasions in which war is not a political instrument, it has been shown that these claims are flawed. This leads to the conclusion that war must have a political motivation behind it and that is what makes war distinct from something like crime.

It can be seen, therefore, that what war is, as Clausewitz points out, 'simply a continuation of political intercourse, with the addition of other means'.[14] This means for an activity to be a war it must have a political context to it. However, what must be noted is that the political aim of war does not have to be to defeat a state: the political motivation can be ethnic or religious, for example. It has also shown that for war to be a war, there must be at least some level of violence to it. Colin Fleming argued that 'War is organized violence threatened or waged for political purposes. That is its nature. If the behaviour under scrutiny is other than that just defined, it is not war'.[15] However, in this author's opinion there needs to be one final element to the definition: there needs to be, as Freeman points out, a severity of threat.[16] This argument can be supported by an analogy. Take for example a student protest. During the protest students riot and attack police officers because they dislike the government's policies towards students. In this scenario, there is clearly a political motivation as well as violence. However, it would not be termed war because of the fact that the threat is not equal to a war. In this way, it is clear that there has to be a substantial level of threat for something to become a war.

For cyber offensive operations to be seen as cyber war rather than something else it would mean that the definitions of what cyber war is would have to meet this definition of war. However, as will be shown below it is clear that this is not the case.

The first way in which cyber war has been defined has been directly related to the military effects. John Arquilla and David Ronfeld were the first to define cyber war. They defined cyber war as:

> conducting, and preparing to conduct, military operations according to information-related principles. It means disrupting, if not destroying, information and communications systems, broadly defined to include even

[14] Ibid., p. 605.
[15] Colin M. Fleming, 'New or Old Wars? Debating a Clausewitzian Future', *Journal of Strategic Studies*, 32:2, (2009), 213-241, 230.
[16] Lawrence Freedman, 'General Introduction', in Lawrence Freedman (ed), *War* (Oxford: Oxford University Press, 1994), p. 1.

> military culture, on which an adversary relies in order to know itself: who it is, where it is, what it can do when, why it is fighting, which threats to counter first, and so forth. It means trying to know everything about an adversary while keeping the adversary from knowing much about oneself. It means turning the "balance of information and knowledge" in one's favor, especially if the balance of forces is not. It means using knowledge so that less capital and labor [sic] may have to be expended.[17]

They further argued that this form of cyber war will lead to a completely new form of war and that it will be to the 'twenty first century what the blitzkrieg was to the twentieth century'.[18] This definition of cyber war has also been, at times, given other labels such as Information Operations by the United States' Department of Defense.[19] However, for clarity, this author will refer this as cyber war. The notion that a definition of cyber war needs a military context is supported by Libicki. Libicki argued that 'operational cyberwar [sic] involves the use of cyberattacks [sic] on an adversary's military in the context of a physical war'.[20] This shows that the term cyber war has been used to describe a situation in which a cyber offensive operation is launched at another country's military.

This definition was also built on by Liff who argued that

> cyberwarfare as a state of conflict between two or more political actors characterized by the deliberate hostile and cost-inducing use of Computer Network Attack (CNA) against an adversary's critical civilian or military infrastructure with coercive intent in order to extract political concessions, as a brute force measure against military or civilian networks in order to reduce the adversary's ability to defend itself or retaliate in kind or with conventional force.[21]

Although this definition does look at targets of attack other than the military, it can be seen that there is an importance placed on attacking the military or having the effect on a country's ability to defend itself. This argument was supported by others such as Marthie Grobler and Joey Jansen van Vuuren who argued that cyber war is a war when it succeeds in 'undermining the quality of opposing force information and denial of service or information collection opportunities to opposing forces'.[22] What

[17] Arquilla and Ronfeldt, 'Cyberwar is coming!', 146.
[18] Ibid., 147.
[19] Department of Defense, 'Department of Defense Directive O-3600.01 Information Operations', 14 August 2006.
[20] Martin C Libicki, *Cyberdeterrence and Cyberwar* (RAND Project Air Force: Santa Monica, 2009), p. 8.
[21] Liff, 'Cyberwar', 405f.
[22] Marthie Grobler and Joey Jansen van Vuuren, 'Collaboration as Proactive Measure Against Cyber Warfare in South Africa', *African Security Review*, 21:2, (2012), 61-73, 62.

becomes clear is that, for these theorists, the military dimension of cyber war is an important part of what makes a cyber war a war. One of the example of this type of activity was during the Kosovo intervention by the North Atlantic Treaty Organisation (NATO) the US launched a cyber offensive operation on the computer systems of the militaries in Kosovo, and some Kosovars also conducted operations against NATO countries.[23] In this way it is clear that, for some, a cyber offensive operation becomes cyber war when it is used against a military system for a military reason.

Nevertheless, it can be argued that there are several problems with relating cyber war solely to the military. This excludes other situations in which the armed forces were not the target or when a war was not already being engaged. However, this is not the biggest problem with these definitions. The main problem with the idea of targeting solely the military is that, it could be argued, when it targets the military or is used when a war is already taking place, it appears that the inclusion of cyber to war becomes redundant. This argument would then lead, it could be argued, that each method of attack in a war would have to be defined as a separate war. For example, if guns were used then it would, if the above argument is followed about cyber war, then it would have to be termed a gun war, and if tanks were used then it would be a tank war, even leading to a point in which if tanks and guns were used then it would have to be termed tank and gun war. It is simply a war. From this, it can be seen that the term cyber is redundant in these cases, and it is just a war. This argument is also supported by the fact that some of the definitions above include the term operation or operational. This then shows that it is not war in itself but a part of war, once again showing that using the term cyber war is redundant. In this way, it could be argued that when a cyber offensive operation is used in support of, for want of a better term, a traditional war, then it should be referred to as cyber operations. In all of these ways, it can be seen that the argument that a cyber war has to directed at the military and that this is what makes a cyber offensive operation into a cyber war is false.

This leads to another area of discussion: the need for a physical effect. It was argued by the US Department of Defense that a cyber event is only war if it

[23] For more information see William M. Arkin, 'The Cyber Bomb in Yugoslavia', *The Washington Post*, first published on 25.10.1999, http://www.washingtonpost.com/wp-srv/national/dotmil/arkin.htm, last Accessed on 25.11.2014, and Chris Nuttall, 'Kosovo info warfare spreads', *BBC News*, first published on 01.04.1999, http://news.bbc.co.uk/1/hi/sci/tech/308788.stm, last accessed on 25.11.2014.

'proximately results in death, injury or significant destruction'.[24] Others support the argument about the need for physical effects for a cyber offensive operation to become a war. For example, it has been argued that, for an attack to become a cyber war, it would need to have an effect on the physical world.[25] To support his view of this idea McGraw argued that an example of this would be gaining control of a piece of military hardware and using that to conduct an attack.[26] He goes on to state that 'in the final analysis, the threat of cyber war is very real but is also grossly overstated'.[27] The ultimate version of this would, of course, be what appears in a lot in both television and films when an organisation takes control of a nuclear power station or a plane.

However, there are problems with this definition. To begin with, one of the problems is actually working out what the Department of Defense definition would mean. For example, the level of death or injury that is needed is not explained. Does it for example mean that there need only be one death from the attack for it to be war? However, as was shown above, a war is more than one act and, in this respect, this definition fails. In addition to this, what is the level of injury that is needed for something to be a war: that is, does it need to be a severe injury or is a minor injury enough for it to be seen as a war? What is 'significant destruction'? Further, the notion of a physical element can also be seen not to work simply because, it could be argued, that if a cyber offensive operation did cause significant damage, death or injury, it seems unlikely that a country would not respond to this with a conventional military attack. It could be argued that if a country responded in a conventional military capacity, then the addition of cyber becomes redundant and it is simply a war. In this way, it can be seen that the need for a physical effect does not work as a definition for cyber war.

There is evidence to support the theory that if a cyber offensive operation was enough to be an act of war, a country would respond in a conventional military manner. For example, in 2011 the US government released the document 'International Strategy for Cyberspace'. In this document it was stated that

[24] Singer and Friedman, *Cybersecurity and Cyberwar*, p. 121.
[25] Gary McGraw, 'Cyber War is Inevitable (Unless We Build Security In)', *Journal of Strategic Studies*, 36:1, (2013), 109-119, 112.
[26] Ibid., 112.
[27] Ibid., 114.

> When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country All states possess an inherent right to self-defense, and we recognize that certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners We reserve the right to use all necessary means—diplomatic, informational, military, and economic—as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests.[28]

This clearly shows that, in the opinion of the US government, if a cyber offensive operation reached the level of threat that would allow it to be termed a war, they would respond in a conventional military way. If this was to happen, then a war would be in place and the use of the term cyber becomes redundant.

Furthermore, in 2008 the UK's Ministry of Defence (MOD) announced that

> The proliferation of [Weapons of Mass Destruction] WMD and [Computer Network Operations] CNO threats means that the UK must have the capability, with its allies, to deter and if necessary defend against or counter such attacks. The UK will require sufficient nuclear deterrent and conventional forces, coupled with intelligence, warning and surveillance infrastructure to counteract potential threats.[29]

From this, it can be seen that, although the statement is less clear than the one from the US, it does directly imply that the UK could respond to a cyber offensive operation in a conventional military way. If this took place, then it would be a war and the term cyber would be redundant. Although it is not clear how other countries would respond to a cyber offensive operation in a similar scenario, it does seem likely that Russia and China would likely respond in a similar manner. This means that the notion of a need for a physical effect for something to be termed cyber war does not work due to the fact that this would lead to an actual war.

A further area that has caused an issue with definitions of cyber war is its relationship to cyber crime. It was argued by Arquilla and Ronfeldt in 1993 that in addition to their cyber war definition (discussed above) that there was another form of cyber activity which they termed as 'netwars'. Netwars, in their opinion

> refers to information-related conflict at a grand level between nations or societies. It means trying to disrupt, damage, or modify what a target population knows or thinks it knows about itself and the world around it.

[28] US Government, 'International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World', May 2011, p. 14.
[29] UK Government, Ministry of Defence, 'Strategic Trends Programme: Future Character of Conflict', p. 32.

> A netwar may focus on public or elite opinion, or both. It may involve public diplomacy measures, propaganda and psychological campaigns, political and cultural subversion, deception of or interference with local media, infiltration of computer networks and databases, and efforts to promote dissident or opposition movements across computer networks. Thus, designing a strategy for netwar may mean grouping together from a new perspective a number of measures that have been used before but were viewed separately.[30]

They then added to their definition of netwars in 2001, stating that 'the term netwars refers to an emerging mode of conflict (and crime) at the societal levels, short of traditional military warfare, in which the protagonists use networks'.[31] This indicates that they felt that crime and war were interchangeable terms. They are not the only authors to do this. This can be seen from the fact that a Russian journal argued that

> isolating cyberterrorism and cybercrime from the general context of international information security is, in a sense, artificial and unsupported ... it is primarily motivation that distinguishes acts of cyberterrorism, cybercrime, and military cyberattacks ... [without knowing the motivation one cannot] qualify what is going on as a criminal, terrorist or military-political act.[32]

It has been argued that the reason why this article included crime within their definition of war was because Russia and China, if not other states, have used criminal groups to conduct cyber offensive operations.[33] In this way, because these states have, at times, outsourced an operation, cyber war has been related to cyber crime. However, this should still be referred to as something other than a crime. This is because a state is still, at some level, controlling the operation as they are the ones who are determine the overall objective of the attack.

In addition to this, it has been argued in an article 'A Corporation Cyber War Strategy' that war and crime are interchangeable terms. The authors argued that a form of cyber war is stealing and using information. They use the term information warfare and define it as 'Actions taken to achieve information superiority by affecting adversary information, information-based processes' and, they add, taking

[30] Arquilla and Ronfeldt, 'Cyberwar is coming!', 144.
[31] John Arquilla and David Ronfeldt, 'The Advent of Netwar (revisited)', in John Arquilla and David Ronfeldt (eds), *Networks and Netwars: The future of Terror, Crime, and Militancy* (Arlington: RAND, 2001), p. 6.
[32] No author given, 'Russian Federation Military Policy in the Area of International Information Security: Regional Aspect', *Military Thought*, 16:1, 2007, no page number given, cited from, Alexander Klimburg, 'Mobilising Cyber Power', *Survival: Global Politics and Strategy*, 53:1, (2011), 41-60, 41.
[33] Ibid., 42.

information.[34] Furthermore, they argue that there are three different types of information warfare:

> Personal Information Warfare where it describes attacks against an individual's electronic privacy. The second type is Corporate Information Warfare; it describes competition, or better said today's war between corporations around the world. The third type is Global Information Warfare, this type of Warfare works against industries, global economical forces or against entire countries or states.[35]

In this way, apart from the last definition, it appears that, to these authors, crime in the use of identity theft and corporate intelligence gathering are types of war. However, there are a number of problems with the above definitions of cyber war. Firstly, the idea of war and crime as terms being interchangeable does not work. To illustrate this argument, it appears that those who include cyber crime as part of cyber war do so simply because of the term 'cyber'. In this, it appears that to these authors the method of doing something is the important part what makes it. That is because cyber crime and cyber war have method of cyber, they must be the same thing. If this were the correct way in which items should be included then it would have to be a similar situation in a 'conventional' situation. For example, because in conventional war they have, for a long period of time, used guns then it would mean that if a criminal group used guns to rob – say a bank – then it would have to be included in war. This is because the method of the crime, that is the gun, was used to rob the bank and guns were used in conventional wars as well. However, this is not the case. This is because all war, whether it is inter-state or intra-state, as was shown above, has political reasons and motivations behind them – this then, is a feature of war. In this way, crime and war are not interchangeable because crime is financially motivated and is not political. Their definitions of cyber war that include crime do not work.

Moreover, the 'A Corporation Cyber War Strategy' article suffers from a similar problem. This is that it appears to confuse intelligence gathering and war. Intelligence gathering is not war and the terms should not be used interchangeably. Again, it appears as if cyber crime and cyber intelligence were placed under the cyber war umbrella because of the fact that the method is the same. This is not the case. To illustrate this, it would be like the simple act of gathering intelligence is the same as a

[34] Amer Nizar AbuAli and Saeb Sisan, 'A Corporation Cyber War Strategy', *GSTF Journal on Computing (JoC)*, 3:3, (2013), no page numbers given.
[35] Ibid.

war in itself. It has been argued in the lead up and during the Second World War, the British using the British Security Coordination gathered intelligence on the United States of America (US).[36] Following the argument put forward about intelligence gathering being the same as a war, then Britain was at war with the US. However, this can be seen to not have been the case. In this way, cyber espionage and cyber war are not the same thing and are not interchangeable simply because, like cyber crime, they use the same method as cyber war.

However, one useful point that these authors do bring forward is that cyber war does not have to be directed at the military for it to be seen as a war. Richard Clarke defined cyber war as 'actions by a nation-state to penetrate another nation's computers or networks for the purpose of causing damage or disruption'.[37] In this, although Clark's argument does allow for the inclusion of the military, it does not state that it has to be directed only towards the military. Moreover, a news article claimed that 'Cyberwar is information warfare waged over the internet. It involves disseminating information via websites or email in order to raise awareness, mobilises support and create global networks of supporters'.[38] This idea has given rise to the claim that it is now possible to defeat the enemy without any fighting being necessary.[39] The author of the article goes on to state that a cyber war allows for the 'enemy to do your will by inducing strategic paralysis to achieve desired ends, and this seizing of the enemy is done almost without any application of physical force'.[40] This argument has further been built on when it has been claimed that it allows the attackers to defeat the enemy without bloodshed.[41] This idea was further supported by the idea that 'cyber warfare should be defined … as the use of exploits in cyber space as a way to intentionally cause harm to people, assets or economies'.[42] Although this definition does contain the idea of harm it also notes that there can be a situation that allows for a war to take place if it damages a country's economy. John Stone

[36] For more information on the British Security Coordination see Nigel West (ed), *The Secret History of British Intelligence in the Americas 1940-1945* (New York: Fromm International, 1999); Keith Jeffery, *MI6: The History of the Secret Intelligence Service 1909-1949*, (London: Bloomsbury, 2010).
[37] Clarke and Knake, *Cyber War*, p. 6.
[38] Giles Trendle, 'Cyberwars: The Coming of the E-Jihad', *The Middle East*, 322:6, (2002).
[39] Amit Sharma, 'Cyber Wars: A Paradigm Shift from Means to Ends', *Strategic Analysis*, 34:1, (2010) 62-73, 62.
[40] Ibid., 64.
[41] David Betz, 'Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed', *Journal of Strategic Studies*, 35:5, (2012), 689-711, 696.
[42] Grobler and Vuuren, 'Collaboration as Proactive Measure against Cyber Warfare in South Africa', 62

supported the argument that economic effects should be included in a definition of war. He argued that during the Second World War the US conducted an air attack on German industry in the Schweinfurt Raid that targeted a ball bearing factory, the destruction of which would have affected the German economy. He argued that because the target in this case was the economy it means that war can be a war even if it tries to target the economy.[43] This is based on the idea that the level of threat that this would cause would be of the level that would justify the term war. However, this seems like an unusual example in itself as the operation took place during the Second World War and as such the event of war was already happening.[44] From this then, to Stone, if a cyber offensive operation targeted economic output, then it could be seen as cyber war.

It appears that what all of these theories have in common is that for a cyber war there needs to be a level of threat. It has been argued that for a cyber offensive operation to become cyber war there need to be a high enough level of threat, which does not have to be caused by targeting the military.[45] This argument is supported by David Rosenfield, who argued that 'it is the disruptive potential of cybernetic attacks, as opposed to their destructive potential, that poses the greatest risk to the security of nations'.[46] The level of threat was further shown when they argued that cyber-warfare is 'an extension of policy (or politics) by actions taken in cyberspace'. They add to their definition by stating that the actions must 'pose a "serious threat" to national security'.[47] They further argued that 'cyber war … is actions taken in cyber space by state or non-state actors that either constitute a serious threat to a nation's security or are conducted in response to a perceived threat against a nation's security'.[48] In this way, it can be seen that the main point of argument in which all of these theorists appear to agree is that for a cyber war to take place it does not have to cause physical harm, but a cyber war is caused when there is a level of threat and then this would allow a cyber war to be deemed to exist.

---

[43] Stone, 'Cyber War Will Take Place!', 105.
[44] Ibid., 107.
[45] James A. Lewis, 'Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats' *Center for Strategic and International Studies*, 2002, p. 4f.
[46] Daniel K. Rosenfield, 'Rethinking Cyber War', *Critical Review: A Journal of Politics and Society*, 21:1, (2009), 77-90, 77.
[47] Paulo Shakarian, Jana Shakarian, Andrew Ruef, *Introduction to Cyber-Warfare: a Multidisciplinary Approach*, (Amsterdam: Morgan Kaufmann Publishers, 2013), p. 2.
[48] Ibid., p. 2.

However, there are problems with these definitions of cyber war based on a level of threat. This is because although the argument that the level of threat changes an attack to war is logical, there is a major failure in this. That is, if a state is feeling so much of a threat that they then consider themselves to be at a state of war, would they not respond to this threat with conventional military force? This argument was supported by Betz.[49] In this way, like in the military context it would appear then that if a cyber offensive operation had the level of threat for a war and a country responded militarily to this, then it would just be war with no need of the addition of the term 'cyber'. If an attack did not have the level of threat for it to be war then it should be referred to as a cyber offensive operation. From this, it is clear that the level of threat that makes war a war does not work as the definition of a cyber war.

Although this chapter has discussed the terms cyber war and netwars as separate terms, what has also become clear is that both types have now been combined in most academic literature. For example, Richard Clark, defined a cyber war as 'actions by a nation-state to penetrate another nation's computers or networks for the purpose of causing damage or disruption'.[50] From this, Clark's definition did not separate the notion of targeting the military or civilian networks.

As was shown above, it is clear that in this author's opinion, none of the definitions that have been presented provide a detailed understanding of cyber war. This is because, although some have looked at the theories of war, others have not even addressed what war actually is. They are not the only people who attempt to define cyber war without defining war, but it does serve as an example. In addition to this, there are those who have discussed theories of war in relation to their definition of cyber war but have produced flawed assessments. For example, Andress and Winterfeld quote both Clausewitz and Sun Tzu, and state that these are applicable to what is happening in cyber space but do not expand on this.[51] From this, it could be argued that, when a theory seeks to term something as war then the first part must always look at what war is. When this has not happened, it can be argued that, it has allowed there to be confusion about what war is and what it is not. For example, the

[49] Betz 'Cyberpower in Strategic Affairs', 696f.
[50] Clarke and Knake, *Cyber War*, p. 6.
[51] Andress and Winterfeld, *Cyber Warfare*, p. 4.

term ‘war’ has been used to describe actions against drugs, crime and poverty.[52] In this way, it has allowed for ‘war’ to become a term in which the meaning has become confused with many other situations, such as crime. It is the author’s opinion that only if something has the characteristics of war should be termed war. This is important in cyber offensive operations because, if they do not have the characteristics of war, then they should not be termed cyber war. This is because if there is no clear definition of something, it could be harder to deal with it. The need to define something to be able to defeat it is something that has appeared time and again. For example, in counter insurgency campaigns, if you term them to be a conventional war and try to fight them as such, it has been shown in a number of cases, that this fails.[53] This, it could be argued, could happen with cyber war. If a person or government does not understand what it is, then how do they go about fighting it? This is why a clear definition of what cyber war is, and by extension what it is not, is so important.

Therefore, for something to be termed cyber war, it is important to first understand what war is: that is for something to be war it must be politically motivated; it must have a level of violence; chance will always be involved; and there must be a level of threat that has high enough severity that would move something from an attack to an act of war. From this, it follows that a cyber war would have to be defined as an action taken by a computer against another computer, that was conducted for a political reason and that had some element of violence as part of it. This violence, it could be argued, would be the action of one computer attacking another, and that the level of threat with that was severe enough for it to be termed war. In addition, the war would have to be confined to the digital side for it to be cyber war rather than war

Although, this thesis has provided a definition of cyber war, the author would also argue that cyber war by this definition is unlikely to take place. There are a number of reasons for this. To begin with, a cyber offensive operation is unlikely to fulfil the definition of war. This is because although a cyber offensive operation might

[52] To see the examples of the use of war in these contexts a simple Google search will demonstrate this situation.

[53] For more information on an argument similar to this see Warren Chin, ‘Examining the Application of British Counterinsurgency Doctrine by the American Army in Iraq’, *Small Wars & Insurgencies*, 18:1, 1-26, and James Pritchard and M.L.R. Smith, ‘Thompson in Helmand: Comparing Theory to Practice in British Counter-insurgency Operations in Afghanistan’, *Civil Wars*, 12:1-2, 65-90, particularly 72.

be politically motivated, it might have some level of violence, that is an action against another system, and a level of chance will always be involved in the abstract version that was offered by Clausewitz, the level of severity is a problem. If a cyber offensive operation were enough of a threat to be considered war then a country that was attacked would respond physically and in a conventional military manner. This would mean that a war was in progress and that the cyber prefix must be removed. To illustrate this it is important to look at one of the claims of a cyber offensive operation. For example, Leon Panetta, former Secretary of Defence stated that 'An aggressor nation or extremist group could gain control of critical switches and derail passenger trains, or trains loaded with lethal chemicals'.[54] However, if this attack happened and it did this, then it is more likely than not that the US would respond, as was shown above, to this attack in a conventional military way. If they did respond to this attack in a conventional way against a country, that country would respond most likely in the same way thus a war. This would then mean that a cyber war was not in progress; a war would be in progress.

This is not to say that a future war would not have a cyber offensive operations as part of it, but that this is not the same as a cyber war. The term for this type of event should be at most a 'cyber operation'. To illustrate this, it is worth looking at an example of when cyber offensive operations have been used in a war. In 2008 it was alleged that Russia launched a number of cyber offensive operations on Georgia after a dispute erupted between Georgia and Russia in a territorial dispute over South Ossetia.[55] These operations have been described by some as being cyber war.[56] The cyber offensive operations were launched in a number of ways, websites belonging to Georgia's Ministry of Foreign Affairs were defaced, and a Denial of Service (DoS) attack on the banking systems and media outlets in Georgia. A DoS attack is when a hacker or a group of hackers overload or shutdown a website. The most common form of a DoS attack is when an attack floods a webserver with requests so it becomes overloaded and shuts down usually using DDoS.[57] This was later followed by a conventional military attack on Georgia by Russian forces. By Russia conducting a

[55] For more information see, David Hollis, 'Cyberwar Case Study: Georgia 2008' *Small Wars Journal*, http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008, last accessed on 12.02.2015.
[56] For example, Richard A. Clarke implies that this was a cyber war in Clarke and Knake Cyber War p. 30.
[57] This will be covered in a lot more detail later on.

cyber offensive operation on the media outlets in Georgia, it meant that Georgia could not contact the outside world about the conventional military attack. However, although this has been termed cyber war, it is in fact a cyber operation that took place within a war rather than constituting a war by itself. To illustrate this, it is worth looking at the same operation but if it was conducted by special forces. If special forces conducted an attack to physically take control of the media outlets to stop them being used to contact the outside world, and then the main military force attacked, what the special forces did would be termed a special operation rather than special war because the attack on its own did not constitute war. This then must be the same for the cyber offensive operation. Therefore, it must in this instance be called a cyber operation.

This then leads to the point that a cyber offensive operation will have a political motivation, a level of violence, an element of chance, but not a level of severity to be termed war. To illustrate this, it is worth looking at a number of cyber offensive operations that happened at the end of 2014. After a period of tension allegedly caused by a Sony film called The Interview, North Korea appeared to have hacked into Sony and released sensitive data.[58] After this, it was alleged that North Korea hacked into a South Korean nuclear power plant and released information about the power station.[59] Finally, North Korea's Internet was shut down, allegedly by the US, although this theory has received criticism.[60] This whole event will be covered in more detail later in the thesis. However, what all of this shows is a confrontation in the cyber environment that was not war. This is because the level of threat was not there for the actions to be deemed a war.

It can be seen that in international law, there is a legal basis for claiming that there can be an act of force that falls below the level of war. To begin with it is worth quoting from the United Nations' Charter. The Charter states, in Article 2 Section 4, that 'All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any

[58] For more information and a time line see BBC News, 'The US has imposed new sanctions on North Korea in response to a cyber-attack against Sony Pictures Entertainment.', *BBC* News, first published, 3.01.2015, http://www.bbc.co.uk/news/world-us-canada-30555997, last accessed on 03.01.2015.
[59] BBC News, 'South Korea Nuclear firm to hold cyber-attack drills after hack', *BBC* News, 22.12.2014, http://www.bbc.co.uk/news/world-asia-30572575, last accessed on 22.12.2014.
[60] For more information see, The Guardian, 'North Korea's internet temporarily blacked out', *The Guardian*, http://www.theguardian.com/world/2014/dec/22/north-korea-suffers-internet-blackout, last accessed on 04.02.2015.

other manner inconsistent with the Purposes of the United Nations'[61] This statement then means that any act of force should not be used against another state. However, it has also been argued, that not all of these acts of force would be war.[62] This argument can be seen when Article 2(4) is compared to Article 51 of the UN Charter. Article 51 states that

> Nothing 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, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.[63]

It is also worth noting that the language contained in these two articles is different. In Article 2, the language is 'threat or use of force' whereas Article 51 states 'the inherent right of individual or collective self-defence if an armed attack occurs'.[64] The change of language is important. This, it could be argued, is clear from the fact of the change of language because if they were the same thing, then the language would be the same in both. This is because an armed attack is a use of force, but not all uses of force are armed attacks. It has been argued that the addition of the use of armed force produces a much narrower definition than the use of force.[65] This then means that Article 51 can only be used by a state 'if and only if, an armed attack has occurred'.[66] This must mean therefore that there is a difference between an act of force and an act of war. What this clearly shows is that an act of force, although not permitted by international law, is not enough to claim that a war is taking place.

To support the above argument it is important to look at the International Court of Justice case looking into a covert action by the United States in Nicaragua in the

---

[61] UN Charter, Chapter I, Article 2, Section 4, http://www.un.org/en/documents/charter/chapter1.shtml, last accessed on 27.11.2014.
[62] Myra Williamson, *Terrorism, War and International law: The Legality of the Use of Force against Afghanistan in 2001* (Farnham: Ashgate Publishing Limited, 2009), p. 105. This argument is also supported by Yoram Dinstein, *War, Aggression and Self-Defence*, Third Edition (Cambridge: Cambridge University Press, 2001), p. 12.
[63] UN Charter, Chapter VII, Article 51, http://www.un.org/en/documents/charter/chapter7.shtml, last accessed on 26.01.2015.
[64] UN Charter, Chapter I, Article 2, Section 4, and UN Charter, Chapter VII, Article 51, Own emphasis added.
[65] Matthew C. Waxman, 'Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)', *The Yale Journal Of International Law*, 36:421, 421-459, 427.
[66] Williamson, *Terrorism, War and International law*, p. 110.

Contra affair that took place in the 1980s. The Contra affair was when the United States provided support to a number of groups which opposed the Nicaraguan government in the 1980s. The importance of this case and the examination of the judgement of the case is that it concerned an act of force that was also a covert action. To begin with, in this case, it was important to look into what an armed attack was. It argued that

> There appears now to be general agreement on the nature of the acts which can be treated as constituting armed attacks. In particular, it may be considered to be agreed that an armed attack must be understood as including not merely action by regular armed forces across an international border, but also "the sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to" (inter alia) an actual armed attack conducted by regular forces, "or its substantial involvement therein.[67]

There are a number of issues that need to taken from this case. To begin with, it is clear from this judgement that a state can only have a claim to the right to self-defence either on its own or as part of a collective self-defence system, if they suffer from an armed attack. In addition, the court saw

> no reason to deny that, in customary law, the prohibition of armed attacks may apply to the sending by a State of armed bands to the territory of another State, if such an operation, because of its scale and effects, would have been classified as an armed attack rather than as a mere frontier incident had it been carried out by regular armed forces.[68]

What this quote clearly shows in that, under international law, there is an assumption that there must be a level of threat from the actions of the group. This clearly shows that if an act falls below this level of threat it must then be something other than an act of war. Finally, the Court argued that

> while the concept of an armed attack includes the despatch by one State of armed bands into the territory of another State. The supply of arms and other support to such bands cannot be equated with armed attack. Nevertheless, such activities may well constitute a breach of the principle of the non-use of force and an intervention in the internal affairs of a State, that is, a form of conduct which is certainly wrongful. But is of lesser gravity than an armed attack.[69]

[67] International Court of Justice, 'Case Concerning Military and Paramilitary Activities in and Against Nicaragua 1986' paragraph 195, p. 93f.
[68] Ibid., p. 93f.
[69] Ibid., paragraph 247.

This then shows that the action of participating in the domestic policies of a group, although it may be an act of force, is again not in itself enough to reach the threshold for an act of war. This is because, from these quotes, there is a clear assumption that there is a threshold of when an action is severe enough to be war. This in interpretation of international law is supported by Yoram Dinstein. Dinstein argued that in international law, there is this assumption about the level of threat.[70] In all of these ways it must be seen that in international law an action by one state against another can be an act of force that is still banned under the United Nations Charter but is not – necessarily – an act of war.

There are a number of points that need to be taken from an application of the evidence presented by the UN Charter and the International Court of Justice to the idea of cyber offensive operations. Differentiating between an act of force and an armed attack in international legal context based on cyber activities is beyond the legal expertise of this author. It would appear that an armed attack would not happen in a cyber situation but this judgment must be left up to legal commentators. However, the main points to take away from the above, is that an act of force is not the same as an act of war. An act of war will also be an act of force, but an act of force will not always be an act of war. Furthermore, as was shown in the International Court of Justice ruling, an act of war will always carry with it an assumption that the action must be of such a level that it would move the actions away from an act of force to an act of war. This means that for an action in a cyber situation to move from an act of force to an act of war, there must be a particular level of threat. But as was argued above, in this author's opinion, if a cyber offensive operation had the level of threat that would justify the term cyber war, then a country would respond in a conventional military way. This would mean a war was taking place and adding cyber becomes redundant. What is left then is that under international law an action can be an act of force but that is not the same as war and this is one reason why cyber offensive operations should be referred to as cyber offensive operations rather than cyber war.

[70] Dinstein, *War, Aggression and Self-Defence*, p. 12.

Understanding Covert Action

Due to the fact that it can be seen that defining cyber offensive operations as cyber war does not work there is a need to reimage their use as something else. This part of the chapter will compare the understanding of covert action to that of cyber offensive operations. Firstly it will assess what covert action actually is. Covert action, or as it is sometimes known, 'covert operations', is defined as 'influencing conditions and behavior [sic] in ways that cannot be attributed to the sponsor' or as 'an activity or activities … to influence political economic or military conditions abroad where it is intended that the role of the … Government will not be apparent or acknowledged publicly'.[71] It was argued that in covert action the target may be able to surmise that a state, say the US, has conducted the operation, but they cannot prove it.[72] It was noted by think tank, The Twentieth Century Fund, that looked into the use of covert action as well as its ability to be used in the future that covert action does not need to be seen as only targeting states but 'covert action means any operation designed to influence foreign governments, events, persons, or organization [sic] which is carried out in such a fashion that it can be plausibly denied'.[73] Although all of these are essentially the same, the important point is that covert action is action intended to change a policy of an adversary, and it is conducted by one state in such a way that another state cannot show who was behind it. From this, it means that covert actions are different from other parts of what states do. Intelligence gathering is about acquiring information, data, or secrets about an adversary with the aim to understand the other's actions or intended actions. Covert action is about changing the adversary's behaviour or policy. Of course, it would also be fair to note that there are times in which a line between intelligence gathering and covert action is blurred. Sometimes, in the process of conducting a political covert action (discussed later) for example, intelligence would be gathered from the human agent who is also conducting the operation. If a state has an agent who is providing intelligence and then the agent decides to try and change the policy of the state, this would be covert

[71] Godson, *Dirty Tricks or Trump Cards* p. xxxi; Lowenthal, *Intelligence*, Fourth Edition, p. 178.
[72] Richard M. Bissell, JR., with Jonathan E. Lewis, and Frances T. Pudlo, *Reflections of a Cold Warrior: From Yalta to the Bay of Pigs* (New Haven: Yale University Press, 1996), p. 209
[73] The Twentieth Century Fund, *The Need to Know: The Report of the Twentieth Century Fund Task Force on Covert Action and American Democracy, with Background paper by Allan E. Goodman and Bruce D. Berkowitz* (New York: The Twentieth Century Fund Press, 1992), p. 31.

action.[74] Although intelligence gathering and covert action are linked, the objectives of the activity are different.

Covert action is also different from other aspects of state behaviour towards other states. This is because it is unacknowledged activity. It is different from normal diplomacy, in which states will use overt means to achieve its ends such as sanctions. In addition, it must be seen that covert action is different not only from war but also from special operations (for example, special forces operations) that take place in war. It was argued the difference between these two activities is the level of secrecy attached. It has been argued that in covert action the 'government's participation is unacknowledged', where as 'clandestine activity [related to special forces operations], … although intended to be secret, can be publicly acknowledged if it is discovered or inadvertently revealed'.[75] This is because it comes down to the idea of publicly acknowledging the use of force. The difference is that when states conduct special operations they do not take active measures to stop other states from being able to show that they were involved in the operation. Take for example Special Operations Executive's operations during the Second World War when they conducted operations, they would at times, intentionally leave evidence that it was the British who had actually conducted the operations. This can be seen in Operation GUNNERSIDE that destroyed Germany's heavy water power plant in Norway.[76]

A further difference is that special operations can be admitted after the operation has taken place. The kill or capture operations of Osama Bin Laden conducted by US Special Forces in 2011 was admitted after the operation had taken place. It could be argued that part of the reason that the US admitted that they conducted the operation after the fact was that one of the helicopters crashed and if it had not, then they would not have admitted it. However, the US had been trying to target Osama Bin Ladin for so long and they felt that if they could show that they had removed him then the level of support for Al Qaeda would diminish. It does go to show that they would have, even without the issue of the helicopter, publicly stated

[74] United States, Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, 'Church Committee Covert Action in Chile 1963-1973: Staff Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities', p. 1.
[75] Marshall Curtis Erwin, 'Covert Action: Legislative Background and Possible Policy Questions', *Congressional Research Service*, 10.04.2013, p. 23
[76] Ray Mears, *The Real Heroes of Telemark: The True Story of Secret Mission to Stop Hiter's Atomic Bomb* (London: Hodder and Stoughton, 2004), p. 164

that they had dealt with Bin Laden. It would then appear that this operation was always going to be publicly disclosed, thus it was not a covert action. This then is a difference between special operations conducted in war and covert action – the acknowledgement of the use of force.

There can also be some issues with the definition of covert action. One of these can be in the terms of 'foreign'. Foreign was included explicitly under the definition offered by the Twentieth Century Fund, but is also discussed in the definition offered by Lowenthal as he states that covert action aims to affect conditions abroad.[77] The issue of the inclusion of the term foreign presents issues for the understanding of covert action especially if covert action was to be used against non-state actors. It must be noted that it is not only through the definition of covert action in which the term foreign has caused an issue. Part of the problem may have been caused by the fact that the first official policy and legal definition of intelligence and covert action came forward in the US in 1947 with the National Security Act. The main target and issue that the US government foresaw itself facing at this time was the Soviet Union, in which case, the term foreign was fine as the targets would have been working for a foreign government or for a foreign organisation.

How the issue of the term 'foreign' can be seen particularly clearly in the case of some of the operations that the British state have conducted. This is because they have conducted operations, which will be looked at below, against the Provisional Irish Republican Army (PIRA). This then presents issues as to understanding what is meant about foreign and when something becomes foreign. For example, is something foreign if the group that is being targeted is working against the British government, or are they still domestic because of where they were born? For example, someone working with the PIRA. If they were born in Northern Ireland they would technically be a British citizen even if they did not class themselves that way, whereas if the person that was being targeted were born in the Republic of Ireland, then they would be 'foreign' even though the members would be working for the same group. This issue has become more relevant when operations have aimed to target the transnational terrorist organisation such as Al Qaeda and the so-called Islamic State as some of the members may again be citizens of the state, looking to conduct the covert

[77] The Twentieth Century Fund, *The Need to Know*, p. 31, Lowenthal, *Intelligence*, Fourth Edition, p. 178.

action against these terrorist groups. In these ways, it is important to understand if covert action could be used against terrorist organisations is an important point.

The author is of the opinion that, in the case of terrorist organisations, the argument must be that if they are working either to subvert a government or working for an organisation which is foreign in terms of where its main base is, then they must be treated as foreign. In this case, a member of IS working in the UK would be classed as foreign rather than being classed as domestic. Further, it is likely that the issue of targeting IS using covert action methods can also be accomplished by targeting members of IS who are outside of the UK. This means that conducting operations which can be seen to be covert action because of how they are structured and the objective of the operation is designed 'to influence … events, persons, or organization', then it must be seen as covert action. The fact that covert action can be used against terrorist organisations and still be covert action is supported by André Le Gallo who has argued for covert action's use in the war of terror.[78] In these ways, just because a state targets a non-state actor does not mean that it is not covert action.

Covert action does not actually account for a large percentage of the work of intelligence agencies. For example, it has been noted that although in the 1950s and 1960s covert action took around half the CIA's budget, when William Casey functioned as Director of Central Intelligence (1981-1987) – which marked one of the other heights in the use of covert action – only around five per cent of the agency's funds were directed towards covert action.[79] Further it was argued that by the 1990s only around one per cent of the CIA's budget was directed towards covert action.[80] Johnson has disputed the figures that Daugherty has offered about the budget for covert action. Johnson argued that a much bigger percentage of the CIA's budget was taken up by covert action activities and programs.[81] However, Johnson's summary is an estimate, whereas Daugherty's appears to be based on access to the budget. Nevertheless, it must also be noted that the number of covert action instances that take place will change from year to year and will reach peaks and troughs depending on

[78] André Le Gallo, 'Covert Action: A Vital Option in U.S. National Security Policy', *International Journal of Intelligence and CounterIntelligence*, 18:2, (2005), 354-359, 356-357.
[79] William J. Daugherty, *Executive Secrets: Covert Action and the Presidency* (Lexington: The University Press of Kentucky, 2004), p. 34.
[80] Ibid., p. 34.
[81] Loch K. Johnson, *America's Secret Power: The CIA in a Democratic Society*,(Oxford: Oxford University Press, 1991), p. 103.

the threats that are perceived to have taken place at individual times. Therefore, if the number is expected, it must also be clear that there is likely to be increases at different times depending on the situation that a particular country finds itself in. This, of course, changes depending on the country that is being assessed and although there is not a complete study of what each individual country does, it is still likely that covert action is a smaller part of intelligence agencies' work than intelligence gathering.

In these ways, it is clear that what makes covert action unique to a state's activity is that firstly: it is used to change a policy, it is used outside of war, and there is a level of deniability to the actions. From this, for cyber offensive operations to be seen as covert action, they must fulfil these criteria.

Cyber Offensive Operations and Covert Action: A Comparison

Covert action is 'an activity or activities … to influence political, economic, or military conditions abroad where it is intended that the role of the … Government will not be apparent or acknowledged publicly'.[82] The definition of covert action is clearly applicable to cyber offensive operations in a number of ways. Firstly, the issue of actions being taken that are not apparent. This has a direct connection with the use of cyber offensive operations. This is because although states do have ways of attempting to identify who conducted a cyber offensive operation, these do have issues. Rid argued that when trying to understand who is behind an operation, a state would look into the method of the operation and the political situation that is happening at the time, to try and establish who conducted a particular operation.[83] By looking into the motivation for the operation, a state would be able to get a very good idea or belief of who was behind an attack. Yet the difference is that this is not the same as proof. It can be seen that cyber offensive operations are being used to target another state without that state being able to prove who was behind it, thus a state has achieved a level of plausible deniability. The argument that this is enough to achieve plausible deniability is supported by the fact that it was argued that although an

[82] Ibid., p. 165.
[83] Thomas Rid and Ben Buchanan, 'Attributing Cyber Attacks', *Journal of Strategic Studies*, 38:1-2, (2015), 4-37.

adversary may be able to surmise that a state was involved in an operation, this is not the same as being able to provide proof for it.[84]

The issue of not being able to prove that a state was behind an operation is one of the reasons that this author believes that Travis Sharp's theory of cyber coercion was flawed in relation to his work on the operation against *Sony Pictures* in 2014 (this will be discussed more in the chapters three and four).[85] This is because North Korea never publicly acknowledged that it was behind the operation against *Sony*. The operation even used another group to conduct it, the Guardians of Peace.[86] By using this other group, North Korea was clearly attempting to allow for a situation to exist where it was able have an unacknowledged use of force, even though everyone was supposed to know that North Korea was behind the operation.[87] In this way, because they are a use of unacknowledged force, cyber offensive operations fulfil one of the criteria of covert action.

In addition to this, it is clear that cyber offensive operations are directly targeting other states, as well as non-state actors, in such a way that the actions are aimed at changing behaviours. This can most clearly be seen in the case of the Stuxnet operation. This is because the aim of this operation was to try and stop the Iranian government from being able to gain nuclear weapons. The timing of the operation falls within the negotiations and the sanctions by the United Nations Security Council. This is because, it has been argued, that the operation began at some point between 2006 and accelerated in 2008 under President Obama. It was argued that the Stuxnet first infected the Iranian system in 2009.[88] In addition, it was argued that the attack that destroyed around a 1000 centrifuges took place between 2009-2010.[89] This follows the pattern of the UNSC negotiations and the UNSC + 1 negotiations that consisted of the US, UK, France, Russian, China, and Germany that

[84] Bissell, *Reflections of a Cold Warrior*, p. 209
[85] Travis Sharp, 'Theorizing Cyber Coercion: The 2014 North Korean Operation Against Sony', *Journal of Strategic Studies*, 40:7, (2017), 898-926, 898-926.
[86] Ibid., 912.
[87] Aspen Security Forum, 'Beyond The Build: Leveraging The Cyber Mission Force Aspen', David Sanger *The New York Times* and Michael Rogers, Director National Security Agency, Commander, U.S. Cyber Command July 23, 2015 Transcript p. 35.
[88] David Albright, Paul Brannan, and Christina Walrond, 'Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report', *Institute for Science and International Security*, published 16 February 2011, p. 1.
[89] Ibid., p. 2.

were working towards the aim of stopping Iran from gaining a nuclear weapon.[90] From this, it is clear that cyber offensive operations fulfil a further part of the definition of covert action – they are being used to influence conditions abroad.

It can also be seen that even if states target non-state actors, these activities are still aimed at influencing conditions abroad. It was as Michael Rogers argued with North Korea targeting *Sony Pictures* in 2014, clearly, an attack on the principles of the US state.[91] This operation then is covert action, just one that targets a non-state actor with the aim of indirectly targeting the US state. In this way, even though North Korea had targeted a non-state actor, the operation was still aimed at influencing the political conditions aboard by targeting a principle of American life. As such, it was covert action.

Lowenthal argued that covert action, is and should be seen to be, a third option between war and doing nothing.[92] In this way, for cyber offensive operations to be covert action they must be used outside of war.

It is clear that in both theories of war and international law itself, there are times when something is a form of aggression against another state, but the aggression does not reach the level of war. The UN Charter has made clear that although states should refrain from becoming involved in each other's internal affairs, unless directly authorised by the UN, if a state does so it will not necessarily mean that an act of war has taken place. This is due to the fact that the level of violence that is created will not reach the level in which a state would be able to justify that an act of war was committed.

This argument is supported by the fact that the International Court of Justice argued that it

> sees no reason to deny that, in customary law, the prohibition of armed attacks may apply to the sending by a State of armed bands to the territory of another State, if such an operation, because of its scale and effects,

[90] For more information on the timing of the negotiations and the sanctions see Moritz Pieper, *Hegemony and Resistance around the Iranian Nuclear Programme* (Abingdon: Routledge, 2017), pp. 1-3.
[91] Aspen Security Forum, 'Beyond The Build: Leveraging The Cyber Mission Force Aspen', David Sanger *The New York Times* and Michael Rogers, Director National Security Agency, Commander, U.S. Cyber Command, 23 July 2015, Transcript p. 35.
[92] Lowenthal, *Intelligence*, Seventh Edition, p. 249.

> would have been classified as an armed attack rather than as a mere frontier incident had it been carried out by regular armed forces.[93]

Further, they argued that 'the supply of arms and other support to such bands cannot be equated with armed attack'.[94] In addition, it was stated that 'such activities may well constitute a breach of the principle of the non-use of force and an intervention in the internal affairs of a State, that is, a form of conduct which is certainly wrongful. However, it is of lesser gravity than an armed attack'.[95] This then means that although a state should not be conducting these actions against another state, they would not be enough, in and of themselves, to justify a claim of an act of war having been committed. In Nicaragua, when both the US and Nicaragua had been involved in covert funding and providing arms to the various foreign forces in the 1980s, it was argued that what turns something from an interference or act of coercion into a something that constitutes an act of war is the 'scale and effect' of the action. In this case then, it is clear that what is being looked at is a case where the actions are being used against a state, but that the actions are not of the level of war – as such there is a need to look for a different way of understanding what these actions are being used for: they are covert action. This is because they are aimed at affecting conditions abroad but the actions are not an act of war.

With the use of cyber offensive operations, it can be seen that the same situation under international law applies. Firstly, even though the case in Nicaragua had focused on traditional forms of attack, in the case of guns and support of terrorists, the same judgement relates to cyber offensive operations. It was argued that the same rules should still apply when it comes to assessing whether something is deemed to be a use of force by cyber means – the actions must be judged against their scale and effect.[96]

This argument was supported by the case of Russia conducting a cyber offensive operation against Estonia in 2007. Estonia had claimed that the cyber offensive operations that targeted them in 2007 were enough to justify the triggering

---

[93] International Court of Justice, 'Case Concerning Military and Paramilitary Activities in and Against Nicaragua 1986' paragraph 247.
[94] Ibid., paragraph 247.
[95] Ibid., paragraph 195.
[96] Micahel N. Schmitt (General Editor) and Liis Vihul (Managing Editor), *Tallinn Manual 2.0 On the International Law Applicable to Cyber Operations: Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence* (Cambridge: Cambridge University Press, 2017), p. 331.

of Article 5 (that an attack against one country would be viewed as an attack on them all) of the North Atlantic Treaty Organisation (NATO) treaty. The Estonian government used language that, it could be argued, tried to show the connections between the cyber offensive operations and traditional military acts. For example, the Estonian Prime Minister tried to equate the DoS activities to a military blockade.[97] However, this was not supported by other members of NATO because it was claimed that the attacks did not meet the level that was needed for it to be seen as an act of war. The argument that it was not an act of war was supported by Rid because the cyber offensive operation could not turn violent, whereas the military blockade could.[98] This then clearly shows that, under international law, it can be seen that states can target one and another without it being war. This means that under international law, actions can take place. This is why having a very clear understanding of the terminology that is being used to discuss these issues is so important and why this researcher has pointed out that cyber war will not take place, both in terms of a terminology of war and the legal arguments.

In addition, it can clearly be seen, as was argued in the introduction, the US and the UK have developed policies that indicate that these two states would conduct cyber offensive operations outside of a war. In the US, The Department of Defense has stated that they will have twenty-seven of the 133 teams dedicated to what they term as 'Combat Mission Teams' that have the objective to 'provide support to Combatant Commands by generating integrated cyberspace effects in support of operational plans and contingency operations'. [99] With the term of contingency operations, it suggests, that these activities would take place outside of war.

In addition, the Department of Defense argued that it 'has developed capabilities for cyber operations and is integrating those capabilities into the full array of tools that the United States government uses to defend U.S. national interests' and that these tools would be used for 'diplomatic, informational, military, economic, financial, and law enforcement tools'.[100] The Department of Defense also argued that they will seek 'to deter attacks and defend the United States against any adversary

[97] Rid, *Cyber War Will Not Take Place*, p. 7.
[98] Ibid., p. 7.
[99] US Government, The Department of Defense, http://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy
[100] US Government, The Department of Defense, 'The Department of Defense Cyber Strategy', April 2015, p. 2.

that seeks to harm U.S. national interests during times of peace, crisis, or conflict'.[101] Furthermore, they argue that

> If directed by the President or the Secretary of Defense, the U.S. military may conduct cyber operations to counter an imminent or on-going attack against the U.S. homeland or U.S. interests in cyberspace … [and that they have] a range of options and methods for disrupting cyberattaks of significant consequence before they can have an impact, to include law enforcement, intelligence, and diplomatic tools.[102]

In this way, it clearly indicates that, in terms of the US, they have developed a policy in that these activities would be used outside of war. This makes these activities covert action.

The British can also be seen to have developed a policy in that cyber offensive operations would be used outside of war. In 2012, the Intelligence and Security Committee argued that cyber offensive operations could take the form of disruption that includes:

> accessing the networks or systems of others to hamper their activities or capabilities without detection (or at least without attribution). The most famous example of this type of cyber activity (although not involving the UK agencies) is the Stuxnet virus which is believed to have caused some disruption of the Iranian nuclear enrichment programme.[103]

In 2015, under the *National Security Strategy and Strategic Defence and Spending Review 2015,* the UK government stated that they would invest a total of 1.9 billion pounds over five years 'to protecting the UK from cyber attack and developing our sovereign capabilities in cyber space'.[104] Although it is not clear, it could be argued that this means that the UK government were developing, with increased funding, the use of cyber offensive operations beyond a simply military strategy. Finally, in 2016, the British government stated that they will use cyber offensive operations as part of a 'full spectrum of capabilities' and they will use them 'at a time and place of our choosing'. [105] This suggests the non-military use of these activities. This means that it can be argued that the UK have developed a policy in which cyber offensive operations would be used outside of war – thus making them covert action.

---

[101] Ibid., p. 2.
[102] Ibid., p. 5.
[103] HM Government, Intelligence and Security Committee, 'Annual Report 2011–2012', published on July 2012.
[104] HM Government, *National Security Strategy and Strategic Defence and Spending Review 2015: A Secure and Prosperous United Kingdom* November 2015, paragraph 4.105, p. 40.
[105] HM Government, 'National Cyber Security Strategy 2016-2021', published 1 November 2016, paragraph 6.5.1, p. 51.

In these ways, it is clear that cyber offensive operations are being done in such a way that they are difficult to trace to an individual state, meeting the idea of non-attributed behaviour, they are aimed at changing a foreign power's behaviour the same as covert action, and finally they are being used as an option in between doing nothing and engaging in war. They are covert action.

Conclusion

This chapter has clearly demonstrated that cyber offensive operations are covert action. To achieve this, it, firstly, had to demonstrate why cyber offensive operations are not, and should not, be seen as cyber war. It found that there is general agreement amongst academics about what covert action is. Although some authors change the odd word around, covert action is defined as 'as an activity or activities … to influence political, economic or military conditions abroad where it is intended that the role of the … Government will not be apparent or acknowledged publicly'. It has argued that this definition not only includes operations conducted against other states, but also against non-state actors such as terrorist organisations.

Using the understanding of what covert action is and what cyber offensive operations are, the thesis found that cyber offensive operations are covert action based on the fact that both types of activities are aimed at changing the behaviour of an adversary. Both types of activities will maintain a level of plausible deniability, and they are not war. From this, it can be concluded that overall a clear relationship between the activities exists based on what they are used for.

Having established how covert action should be defined and the types of operations that usually take place as part of a covert action campaign it can be argued that the relationship between covert action and cyber offensive operations could be established if the types of operations are the same, if the way they are being conducted are similar, if the actions are less than war, and if the actions are unacknowledged. The next two chapters of the thesis will examine whether this is the case.

CHAPTER TWO

Covert Action and Cyber Offensive Operations: A Comparison between Propaganda Activities.

The next three chapters will compare the types of activities that are considered to be covert action to those that can be seen to have taken place using cyber offensive operations. This is because, although this author believes that in terms of understanding the operations in general both have clear similarities it is also important to compare the types of activities that are seen as covert action to their cyber offensive equivalent. These chapters will look at the types of covert action activities that have taken place. It will do this by comparing the various ways that academics have described about the types of activities that constitute covert action. Some, for example Harry Rositzke and Gregory Treverton, argue that there are three types of covert action: propaganda, political, paramilitary. [1] This though misses out economic operations that Lowenthal argued were separate forms of covert action.[2] There are some logical reasons for not having economic activities as a separate form. This is because economic activities can, at times, be directly linked with political, in the sense that, if a state looks to affect the economics of a particular group, it is more likely affect its political stability. In addition, there have been operations that have provided economic support to a particular political party and therefore, as will be shown in greater detail below, there is a blurred line between economic activities and political activities. Yet others, for example Mark Lowenthal, argue that there are five overarching forms of covert action: propaganda, political, economic, coups, and paramilitary.[3]

This author has chosen to treat economic operations as a separate form of activity in order to highlight them as having their own uses, rather than simply being part of political operations. In addition, the author has also chosen to follow the lines of Mark Lowthental, who begins his discussion of covert action by looking at the least violent forms – propaganda – and then moves towards the most violent – paramilitary.

[1] Harry Rositzke, *The CIA's Secret Operations: Espionage, Counterespionage and Covert Action* (London: Westview Encore Edition, 1988); Gregory Treverton, *Covert Action: The CIA and the Limits of American Intervention in the Post Cold War World* (London: I.B. Tauris, 1987).
[2] Lowenthal, *Intelligence*, Fourth Edition, p. 178.
[3] Lowenthal, *Intelligence*, Fourth Edition, p. 178.

Using these types of activities as a basis the author will argue that there are four overarching ways that covert action can be seen to take place. These are: propaganda, political, economic, and paramilitary. This chapter will look at the use of coups, but unlike Lowenthal it will discuss these in relation to political activities. This is because this author feels that coups are a political activity rather than something else. These chapters will also argue that these overarching forms of activity can also be seen to have taken place or could take place using cyber offensive operations The direct relationship between cyber offensive operations and covert action will be addressed in chapter five after the author has highlighted the types of activities that can be seen to constitute cyber offensive operations in the preceding chapters. This is because – as the author will argue in chapter five – these operations should not be seen as a separate form of activity. For each of the forms of covert action, the chapter will provide an account of this type of activity, and examples of when each form activity can be seen to have been used in the past. It will not aim to provide a complete account of every instance of the use of covert action. This is because this would be too big a study for this chapter to achieve. However, there have been such studies conducted in the past.[4]

The other aims of these chapters are to provide an empirical assessment of the ways that cyber offensive operations are being conducted by states. However, this presents a number of issues. Firstly, there is a problem of attributing an operation to a particular state. This is because cyber offensive operations can be conducted through using a group or groups that have alleged links to a state to conduct an operation rather than a state's own organisation. This means that, although it may appear to have been conducted by one state against another, it could be that a particular group acted without instructions or knowledge of a state. Although the author will highlight these cases, to show that the operation may not have been connected to a state, there is a danger that some of the operations that have been linked to a particular group may not have been conducted by them directly or indirectly. However, all care will be taken to avoid this. Nevertheless, the danger of this issue will, to some extent, be

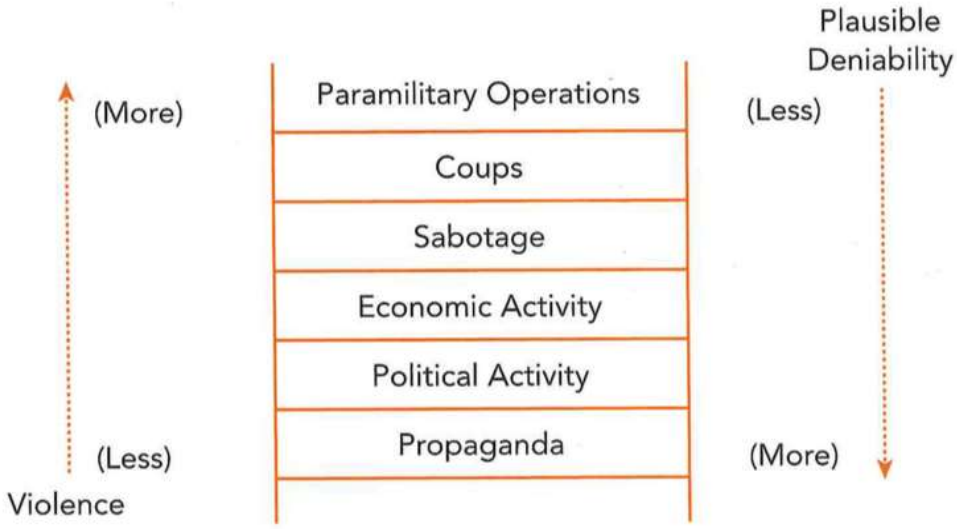
[4] For a good account of various historical examples of covert action see Richard J. Aldrich, *The Hidden Hand: Britain, American and Cold War Secret Intelligence* (London: John Murray, 2001);,Stephen Dorril, *MI6: Fifty Years of Special Operations* (London: Fourth Estate, 2001); Daniel W.B. Lomas, *Intelligence, Security and the Attlee Government 1945-1951 An Uneasy Relationship?* (Manchester: Manchester University Press, 2017); James Callanan, *Covert Action in the Cold War: US Policy, Intelligence and CIA Operations*, (London: I.B.Tauris, 2010).

mitigated by the second objective of these chapters, which is to examine how cyber offensive operations could be used by states. This means that, by showing the ways that cyber offensive operations have taken place, even if these were conducted by a proxy organisation, or have been misidentified, it will still clearly show the ways states could use these operations in the future.

The three chapters that will follow the idea of Johnson, Daugherty, and Lowenthal who argue that covert action methods follow a ladder of escalation in which operations can be judged to be a higher violation of international law, or as Lowenthal argued, more violent.[5] This ladder of escalation will also be shown to exist with the use of cyber offensive operations. Others take a different approach to how they evaluate covert action and its forms. James Callanan argued that academics should break down covert action according to the reason the operations were launched rather than the method of the operation. Callanan argued that there were three reasons for the use of covert action. Firstly, there are defensive covert actions: this is where the operations are launched to defend a US ally. Secondly, offensive covert action is where the actions are undertaken to destabilise a communist regime. Finally, there is preventative covert action that is used to stop a country from turning unfriendly.[6] Although this is an excellent way to understand the reasons a state might use covert action, it does not clearly illustrate the various forms of covert action.

[5] Loch K. Johnson, *Secret Agencies: US Intelligence in A Hostile World* (New Haven: Yale University Press, 1996), p. 61, Lowenthal, *Intelligence*, Fourth Edition, p. 178.
[6] Callanan, *Covert Action in the Cold War*, (London: I.B.Tauris, 2010).

Figure 2: Mark Lowenthal's Covert Action Ladder.[7]



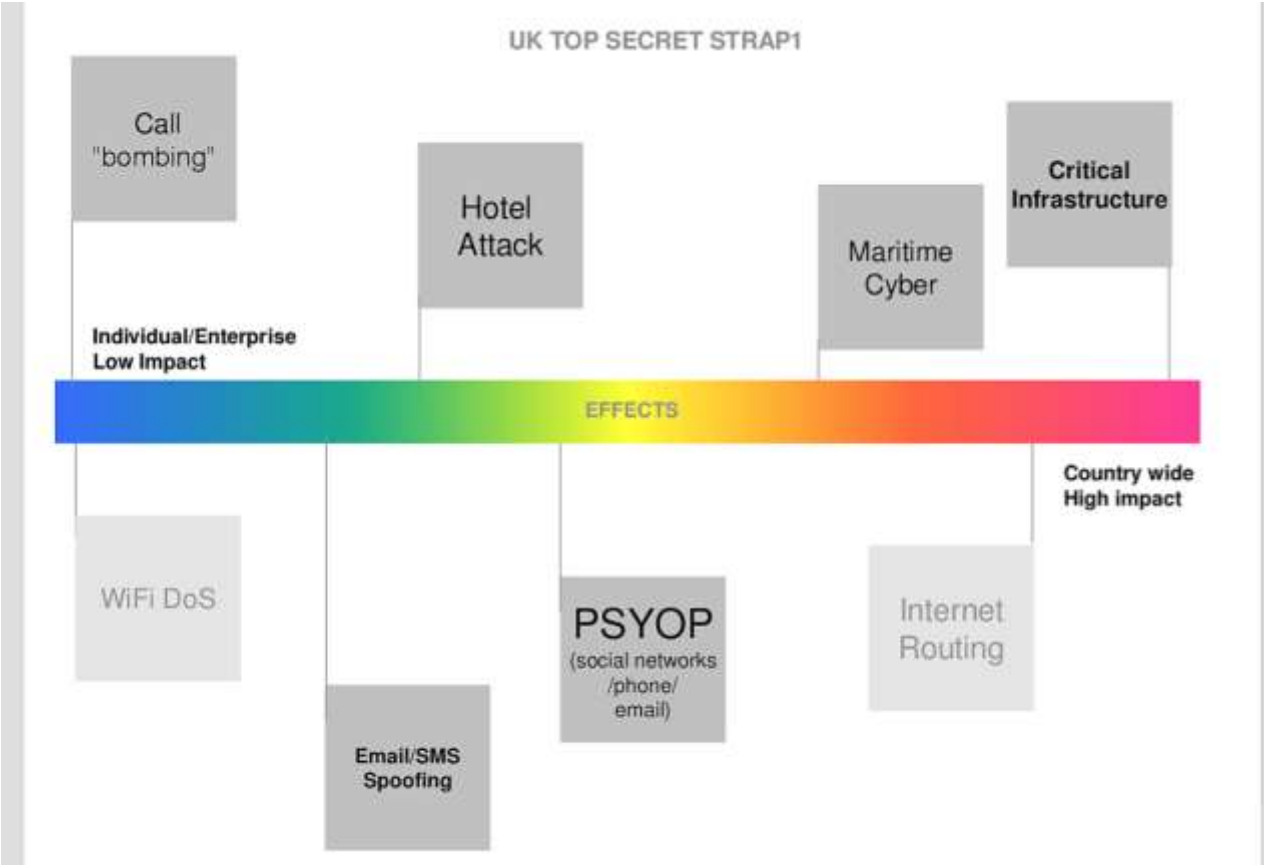
Although this model could be seen to be flawed because, as Lowenthal notes most covert action campaigns will use a multitude of types of activities, it does serve as a useful tool to illustrate the levels of covert action and the threat they pose. Not only does it show the level of threat, it also clearly shows that the more violent the operation is, the more likely it is that the operation and the state that is conducting it will become known.

As was the case with the traditional forms of covert action, it is clear that, in some ways, dividing up operations into forms of activity is a little artificial as complete cyber offensive operations campaigns will often use many different types of activities to achieve the goals of the campaign. For example, a political cyber offensive operation will most likely, as a component of the campaign, include propaganda as well. However, there are two benefits to breaking down these operations in to the forms of activity. Firstly, it allows for a clear understanding of these operations. Secondly, by structuring the chapter in this way, it allows it to follow the idea that operations follow a hierarchy of violence. This theory is based on the work of Herman Kahn who argued that in relation to international crisis there is a hierarchy of the actions of states.[8] This hierarchy was then used to create the covert action that, as was argued in the second chapter, was used to evaluate the violence of

[7] Lowenthal, *Intelligence*, Seventh Edition, p. 257.
[8] Herman Kahn, *On Escalation: Metaphors and Scenarios*, (Westport: Greenwood, 1986), p. 38.

covert action.[9] The level of violence is not linked to the number of people affected, as was claimed to be the case in documents contained in a GCHQ file released by Edward Snowden (see below). The level is, instead, linked to the violence of the operation. Using the notion of violence, the author will clearly examine four forms of cyber offensive operations.

Figure 3: GCHQ's Effects Hierarchy.[10]



In this chapter, the author will compare the form of covert action that is argued to be propaganda to the same forms of action that can be seen to take place using cyber offensive operations. It will begin with an assessment of propaganda that can be seen to take place during the Cold War This activity will be compared to propaganda that can be seen to have taken place using cyber offensive operations. This chapter will also argue that a 'new' type of cyber offensive operations as compared to covert action is direct counter propaganda. This chapter will demonstrate what direct counter propaganda is and examples of its use.

[9] Johnson, *Secret Agencies*, p. 61.
[10] Edward Snowden Document, GCHQ, 'Full Spectrum Cyber Effects SIGINT Development as an Enabler for GCHQ's "Effects" Mission', ca.2010, p. 6, Snowden Surveillance Archive.

This chapter will argue that when the use of propaganda as a form of covert action is compared to propaganda using cyber offensive operations, there is a direct connection between the two. Further, it will argue that overall propaganda using cyber offensive operations are not in fact new as a form of activity. It will argue that anything that is 'new' with cyber offensive operations in this form of activity is simply using a different method to achieve the same type of activity.

Traditional Covert Action: Propaganda

The first way in which states can conduct covert action is through the spreading of propaganda. David Willcox defined propaganda as 'the conscious or unconscious attempt by the propagandist to advance their cause through the manipulation of opinion, perception and behaviour of a target group'.[11] It has been argued that there are three types of propaganda: white, grey, and, black.[12] Propaganda could be spread through the creation of booklets, articles, or even with the creation of organisations that have the aim of promoting a particular country. This is something that is, for the most, part un-troubling in the general behaviour of states as most states actively to a varying degree take part in these types of activities, and it is usually the case that this is almost considered to be something that is normal. However, the aim of propaganda that is being discussed here is more than that, it is usually not just aimed at getting support for a country but is actually designed to get some form of action. This has been termed white or overt propaganda. Then, there is grey propaganda. This is where the information is largely true but the organisation that is spreading the information is not known or has at the very least a thin veil of cover for the organisation. Finally, there is black propaganda. This is where the information is false and the organisation that is spreading the information is not known. It could be argued that white or overt propaganda is actually not covert action. This is because the person, organisation, or even the country disseminating the propaganda is known and the information is true. However, as Daugherty has argued, white propaganda can still be a form of covert action, in the sense that an intelligence organisation can give the report to a friendly journalist and let them identify the source but make sure there is a slant to the report.[13]

[11] David R. Willcox, *The Press and Conflict: The Gulf War and Kosovo* (London: Routledge, 2005), p. 21.
[12] Daugherty, 'The Role of Covert Action', p. 282f.
[13] Ibid, p. 282f.

This, then, shows that propaganda covert action has a number of different methods to achieve its goal.

Propaganda can be spread in a number of different ways. It can be spread through news organisations, for example by giving information to a particular news agency or a journalist so that they can be used to spread the propaganda. It has often been hoped that after giving the story to one news organisation, other news organisations would pick it up and spread the story. One example of this took place in 1949 when the British were able to get a story spread about forced labour camps in the Soviet Union. The information was spread to a few news organisations and then was spread as more organisations saw the information.[14] It was argued by Breckinridge, that having a story reprinted in other news outlets allows a story to have stronger credibility.[15] By conducting a propaganda activity in this way, a covert action operation can reach a lot more places than just by targeting a particular organisation. This then makes it cost effective in both a financial sense and labour cost.

Further to printed media operations, it has also sometimes been possible to take control of an entire media outlet. This has been seen to have happened in the case of US involvement in Chile from 1956 until 1970 when a news organisation was denied funding because of the information that this organisation was spreading. It was then bought by the US and used to spread the information.[16] By taking complete control of a media organisation, a government in one country can have a lot more control over what is printed in another because there would be more journalists that they could use Of course, this can be clear to another government that this has happened as this internal government has stopped providing money so it will be clear to them that someone is supplying the money. However, it is possible that they could secretly fund a smaller part of the news organisation. This means that they may not have as much control but it could be less clear than having another government funding an entire organisation.

---

[14] All references are to documents held at The National Archives (TNA): Public Record Office (PRO), Kew, unless otherwise stated. TNA, CAB 134/3, 'Official Committee of Communism Overseas', Progress Report: Information Research Department, 1st January to 31st July 1949, Forced Labour Codex, Annex C,

[15] Scott D. Breckinridge, *The CIA and the US Intelligence System* (Boulder: Westview Press, 1986), p. 221f.

[16] United States, Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, 'Church Committee Covert Action in Chile 1963-1973 Staff report of the select committee to study governmental operations with respect to intelligence activities', p. 8.

In addition, propaganda has been spread by radio. This has been used in the past to spread information both real and fake to populations. The first way in which radio broadcasting has been used to spread propaganda is through the creation of radio platforms that broadcast into other countries. This was done throughout the Cold War with the US using Radio Free Europe and Radio Liberty. Radio Free Europe transmitted radio broadcasts into Soviet controlled Europe and its sister service, Radio Liberty transmitted into the Soviet Union.[17] It was argued that both of these stations were directed towards peacefully dismantling the Soviet Union.[18] Goodman argued that one of the CIA's covert action successes was in bringing information into the Soviet Union.[19] A further way it has been used is 'ghosting', which means taking control of hostile frequencies to spread certain messages.[20] Further, a way of conducting radio propaganda similar to that of ghosting is snuggling, in which radio broadcasts were on a frequency directly adjacent to the target's own radio broadcast. This was done in the hope that people might accidently listen in to the broadcast, or believe that they were actually listening to the target's broadcast.[21] It has been argued that one of the most successful groups to use this technique was the Solidarity movement in Poland during the 1980s.[22] In this way, it is possible that an organisation can get people to listen to the broadcast thinking that it actually belongs to a different group.

Finally, organisations can use people to spread propaganda. This can be through spreading rumours or organisations can use academics to spread information. It was argued by Breckinridge that the CIA would commission and distribute scholarly work that the CIA believed would be of interest to the Third World.[23] The aim was to get someone to spread a certain piece of information to the target population who would believe it. This is different from the other rumours that will be looked at later because of what the activity is hoping to achieve. The aim is not to target some part of the political element of a government, at least not directly, or

[17] Arch Puddington, *Broadcasting Freedom: The Cold War Triumph of Radio Free Europe and Radio Liberty* (Lexington: University of Kentucky Press, 2000), p. ix.
[18] Ibid., p. x.
[19] Melvin A. Goodman, 'Espionage and Covert Action', in Craig Eisendrath (ed), *National Insecurity: U.S. Intelligence After the Cold War* (Philadelphia: Temple University Press, 2000), p.27
[20] Godson, *Dirty Tricks and Trump Cards*, p. 152.
[21] Ibid., p. 152.
[22] Ibid., p. 152.
[23] Breckinridge, *The CIA and the US Intelligence System*, p. 222.

create issues in the economy but it is to get the population to think their government is doing something that is not in their interest.

The type of information that a propaganda operation spread depends more on what it is hoped it will achieve. The information could be true but come from a source that is connected to a different government. This can be the equivalent of creating a rival news broadcast to highlight an aspect which one government does not want to be known to the general public but another government wants them to know. The use of a propaganda operation to tell the truth has been argued to be the most successful form of propaganda operations.[24] Propaganda operations can also spread information that is false. One of the most notable examples is when the Soviet Union spread the story that HIV was created by the Americans as part of a biological warfare campaign. It appears that this operation began in 1984 and it was argued that by 1987 around forty different countries covered it as a major story.[25] This propaganda operation was so successful that to this day, it still appears every so often.[26] In addition, sometimes information itself is not needed. One of the US campaigns against Iran in the lead up to the coup in 1953 was conducted by the CIA's art department. This department came up with cartoons that which were anti-Mossadeq.[27] Mohammed Mossadeq was the Iranian Prime Minister, who maintained nationalist beliefs. This annoyed the British due to the fact that Mossadeq had nationalised the Anglo-Iranian Oil Company. This meant that the money coming from this company would not be as much as the British government had wanted. This meant that the British had wanted to indicate that Mossadeq was turning towards and was seeking to create an Iranian communist country.[28] In these ways, it is clear that propaganda can take a variety of forms.

However, there have been times in which it can be seen that states have used propaganda to conduct covert action against non-state actors such as terrorist organisations. The British have sought to conduct propaganda operations against non-state actors. For example, it has been claimed that the British conducted various

[24] Daugherty, 'The Role of Covert Action', p. 282.
[25] Christopher Andrew and Vasili Mitrokhin, *The Mitrokhin Archive II: The KGB and the World* (London: Penguin, 2006), p. 400 and p. 466.
[26] William Daugherty 'The Role of Covert Action', p. 282.
[27] The National Security Archive, Dr. Donald N. Wilber, CIA, Clandestine Services History, *Overthrow of Premier Mossadeq of Iran: November 1952 - August 1953*, March 1954, p. 20.
[28] Richard J. Aldrich and Rory Cormac, *The Black Door: Spies, Secret Intelligence and British Prime Ministers* (London: William Collins, 2016), p. 174.

propaganda campaigns against the PIRA. It was argued that the British had looked to 'overtly and covertly, to blacken the IRA'.[29] These have ranged from white operations in such a way that the army set up a press office and worked day and night by 1971. The army was so effective at setting up these press offices that, it has been argued, this became the one of the most popular sources of information for journalists.[30] In this case, this was clearly a white propaganda as the journalist 'knew' who the information was coming from. It was not only through the use of white propaganda that states have looked to target non-state actors. To conduct a covert black propaganda campaign against the IRA the British government set up the Information Policy Unit in 1971.[31] The organisation had help from the Secret Intelligence Service as well as the Information Research Department that conducted propaganda for the Foreign Office. It has been argued that some of the stories that this organisation spread suggested that there were connections between the IRA and the Soviet Union.[32]

There are a number of issues with the use of propaganda. The first issue is that for this type of activity to be successful the information must come from – or appear to come from – somewhere where it can be believed, otherwise, it will be of no use. At times, there may be no need to do anything other than create a rival propaganda machine to that of the adversary if the people in the country you are trying to target do not believe the information that is coming from their own government. At other times it has meant that organisations have been forced to try and find people who dislike something in their own country and then support these people to try and spread propaganda. This was acknowledged by the British government in the 1950s when the Committee for Communism Overseas started to look at setting up propaganda operations that target both Communist China and the Far East in general. They understood that if any propaganda operation was going to be successful, they would have to make sure that the propaganda could be linked to someone who was supported by the people in China rather than someone who was clearly British or

[29] Ibid., p. 174.
[30] David Miller, *Don't Mention the War: Northern Ireland, Propaganda, and the Media* (London: Pluto Press, 1994), p. 78.
[31] Ibid., p. 78.
[32] Paul Lashmar and James Oliver, *Britain's Secret Propaganda War 1948-1977* (Stroud: Sutton Publishers, 1998), p. 156.

clearly worked for them.[33] This is because, if it was clear that the propaganda was coming from the British or any other western government, then they argued it would not be believed. This is why the British were searching for a person who was supported by the Chinese population. It is not clear from the documents whether the British were able to find such a person, but it does show that any government seeking to conduct propaganda activities must take into account whether the information that they are spreading is likely to be believed if it is clear that it is coming from a government or whether they need to make sure that it is hidden that they are conducting the operation.

Another issue when conducting a propaganda campaign is making sure that all groups that conduct the propaganda activity follow the policies that have been set and that they all follow a coherent strategy going forward. Although this may seem easy, due to the fact that, in terms of states, there are, at times, many different organisations which conduct similar if not identical roles. If there are many different organisations that are looking to conduct certain campaigns, there is a danger of having different priorities. This can be seen in the fact that during the Malayan Emergency, there was a disagreement between the Colonial Office and the Foreign Office as to what should be put forward. For example, there was a disagreement as to whether the Malayan insurgencies had connections to the Soviet Union and what these connections were.[34] This meant that there was an issue about whether the propaganda directed towards Malaya should highlight this. In addition, there was no agreement about the language that should be used in the campaign, whether the groups should highlight the Chinese ethnicity of the insurgents, or even whether the group should be termed terrorists or bandits. This is a situation that states who are looking to conduct a propaganda campaign should try and avoid. They should look to create a clear message and have all groups, whether they are conducting white, grey, or black propaganda, have a clear set of ideas about what they should highlight. Although this operation was not directly covert action as the level of deniability was not there, it does demonstrate some of the issues with covert action propaganda.

[33] TNA, CAB 134/3, 'The Official Committee of Communism (Overseas)', The Official Committee of Communism (Overseas) The Cold War in the Far East A.C. (0) (50) 31, 19.07.1950, p. 4.
[34] Susan L. Carruthers, *Winning the Hearts and Minds British Governments, the Media and Colonial Counter-Insurgency 1944-1960* (London: Leicester University Press, 1995), pp. 75-87

It is apparent therefore, that from the perspective of traditional 'forms' of covert action, there are many ways in which a propaganda covert action campaign can be pursued. Overall, the only limit is that the actions must maintain some level of plausible deniability. It is equally apparent that propaganda has been used in many operations.

Cyber Offensive Operations: Propaganda

It is clear that states have used a cyber offensive operation in a number of different ways. One of the first ways that cyber offensive operations have been used by states is through the use of social media to conduct propaganda. Much in the same way that the propaganda activities were discussed above, there are white propaganda cyber offensive operations campaigns that use social media as a platform. This is where a state admits that it is using social media to spread information that is true.

It is clear that Britain has conducted this type of operation. One example is when British diplomats in Russia and Ukraine regularly released photographs of Russian-supplied heavy weaponry from 2014 onwards.[35] This was to highlight the Kremlin's role in the conflict in the Crimea between Russia and Ukraine. The British have looked to expand this operation. This can be seen in the fact that the former Foreign Secretary Philip Hammond (2014-2016), stated that Britain might broadcast the financial secrets of Russia's ruling people. This was to target the people who have helped Vladimir Putin, President of Russia, to stay in power.[36] The British use of *Twitter* is related to the sanctions that the EU and the US have put in place against Russia in response to Russia's involvement in Ukraine. It would appear to be aimed at showing the people of Russia and the world that, while the Russian people are poor, the President of Russia and his associates are rich and are getting richer and it is possible that they have engaged in criminal activity. The aim of this type of operation is to create discontent within the people of Russia that, while they are suffering from the sanctions, the President and his associates are not losing out to the same extent as ordinary Russians.

---

[35] Matthew Holehouse, 'Britain may broadcast Putin's financial secrets to Russian people', *The Telegraph*, first published, 10.03.2015, http://www.telegraph.co.uk/news/worldnews/europe/russia/11461163/Britain-may-broadcast-Putins-financial-secrets-to-Russian-people.html, last accessed on 10.03.2015.
[36] Ibid.

The use of social media to spread white propaganda has not just been directed against other states. A number of operations have used cyber offensive operations to direct propaganda towards terrorist organisations. The US State Department has used *Twitter* as a way to target those who were thinking about joining IS. It has been argued that one of the ways that an operation like this has taken place is through the Center for Global Engagement (in January 2016, this organisation changed its name from the Center for Strategic Communications). The Center for Global Engagement stated that it would take part in targeting a foreign audience via social media to target people who are believed to be becoming radicalised and are looking to join terrorist organisations. It has been stated that they were 'supported by people who are called digital outreach specialists who are fluent in Arabic, Urdu, Punjabi and Somali to counter the work of terrorist organisations'.[37] It has also been stated that the same groups had also worked in English and that they had targeted English language websites to further reach terrorist organisations' recruits.[38] It has been argued that there were more than three hundred and fifty US State Department social media accounts operating from various points that were being used to spread propaganda directed towards people who are looking to join terrorist organisations.[39] It was argued by Aistrope, that this programme allowed the US to use social media to be more persuasive towards a target audience.[40] Amble also argued that using social media to demonstrate important aspects of US financial help in the Middle East would go a long way in helping against terrorism.[41] This then shows that states have conducted propaganda cyber offensive operations that target terrorist organisations by conducting social media campaigns against terrorist organisations.

However, there are a number of issues with these types of white propaganda campaigns. To begin with, by posting the message on *Twitter* from government sources, it is perfectly clear who is conducting the operation. Even if the campaign does not use 'official' government accounts and only uses the 'private' *Twitter* feeds

[37] Eric Schmitt, 'U.S. Intensifies Effort to Blunt ISIS' Message', *New York Times*, first published on 16.02.2015 http://www.nytimes.com/2015/02/17/world/middleeast/us-intensifies-effort-to-blunt-isis-message.html?hp&action=click&pgtype=Homepage&module=first-column-region&region=top-news&WT.nav=top-news last accessed on 17.02.2015
[38] Ibid.
[39] Ibid.
[40] Tim Aistrope, 'Social Media and Counterterrorism Strategy', *Australian Journal of International Affairs*, 70:2, (2016), 121-138, 131.
[41] John Curtis Amble, 'Combating Terrorism in the New Media Environment', *Studies in Conflict & Terrorism*, 35:5, (2012), 339-353, 346.

of the embassy or state department official, it would still be perfectly clear who has sent the information. In addition, if the target population is hostile towards the particular country that this account is connected to, they may view this activity simply as a state sending out the information that is a lie. Further, by using *Twitter* in this way, the message will only reach those who follow the person who posted the information. Although a message can be promoted by the use of re-tweets, as this may allow the message to reach further audiences, it would still only really reach a small number of people. This means that an operation that is directed like this will most likely only reach those who already believe the message and are looking for information to support their view. In this way, this activity is less likely to have the ability to sway a large proportion of a population to a particular point.

However, this type of operation must clearly have some merits. Firstly, the benefit of conducting white propaganda via *Twitter* is that because people know the person that is stating these views, it may mean that people think it is more likely to be true because the government being associated with it has developed trust. Further, a white propaganda operation could also be used as a way in which information could be picked up by other organisations such as a news organisation that could then spread the information further. In addition, this is clearly one of the simplest forms of cyber offensive operations and could be conducted by states in terms of technological aspects. Although some may argue that this is not an offensive use of cyber as it is overt, it clearly is. This is because a cyber offensive operation is looking to produce an effect in the real world. This operation is used to change the behaviour of people. Therefore it is a cyber offensive operation.

However, it is clear that states have also developed other ways to use social media in a more covert manner that allows it to be used to spread a message where it is not known from whom it is coming. The information in this case can either be true or untrue depending on the objective of the operation. Even with this type of operation, there are a number of ways to conduct it.

One way is what can be termed human directed operations. These are operations controlled by humans. A way that a state could do this, and Russia has allegedly done, is through employing people with the sole purpose of spreading

information on various social media platforms.[42] There are clear indications that Russia has been using cyber offensive operations for a propaganda campaign in Ukraine. It has been argued that Russia has developed a cyber offensive campaign that targets the Russian speaking population of the Baltic States with the aim of trying to convince the populations based there that they should not support the European Union or NATO.[43] It became clear in an interview conducted by *The Independent* with a Russia citizen who worked within this campaign that Russia had set up a special group that would conduct an online campaign designed to use the social media. Within this interview, a former member of a team that was designed to do this stated that they worked in an organisation that was state-sponsored, designed to post pro-Putin propaganda on news and social media websites.[44] Although this person seemed to be involved, not in the social media side but involved in news forums (will be discussed later), he states that Russia had set up teams whose sole purpose was to promote stories that Russia wanted promoted.[45] From this, social media was used as a platform to spread propaganda.

This type of operation has been used or, at the very least developed, for use against terrorist organisations. It has been argued that the British have begun an operation in which they would select young Muslims who live in Egypt to be given intensive English language training so that they can blog and tweet against terrorist organisations.[46] This then goes to show that the idea of using other organisations and people without direct noticeable connections to western governments would be used to spread propaganda. In this way, cyber offensive operations can take place on platforms such as *Twitter* and clearly, are taking place and they are being used both by states against other states but also against terrorist organisations.

---

[42] Maria Hellman and Charlotte Wagnsson, 'How can European States Respond to Russian Information warfare? An analytical framework', *European Security*, 26:2, (2017), 153-170, 156, and Bettina Renz, Russia and 'hybrid warfare', *Contemporary Politics*, 22:3, (2016), 283-300, 290.
[43] Chris McGreal, 'US set to revive propaganda war as Putin's PR machine 'undermines' Baltic states'', *The Guardian*, first published 25.04.2015, http://www.theguardian.com/world/2015/apr/25/us-set-to-revive-propaganda-war-as-putin-pr-machine-undermines-baltic-states, last accessed on 25.04.2015.
[44] Paul Gallagher, 'Revealed: Putin's army of pro-Kremlin bloggers', *The Independent*, first published on 27.03.2015, http://www.independent.co.uk/news/world/europe/revealed-putins-army-of-prokremlin-bloggers-10138893.html, last accessed on 28.03.2013.
[45] Ibid.
[46] Kunal Dutta, 'Isis is winning the digital propaganda war, says extremism expert', *The* Independent, first published on 20.02.2015, http://www.independent.co.uk/news/world/middle-east/isis-is-winning-the-digital-propaganda-war-says-extremism-expert-10059200.html, last accessed on 20.02.2015.

A further way that an operation like this has taken place is through the development of operations where a message is created with the sole intention of becoming viral. GCHQ has, according to the Snowden files, developed this type of activity. GCHQ were given the objective through JTRIG to develop messages that would go viral. They supposedly used *Twitter*, *Facebook*, *YouTube*, and *Flickr*.[47] GCHQ also suggested that they had the ability to shape a message based on the specific locations of users and this had a high degree of cognition.[48] What this clearly shows is that one way that information is being spread is through the use of either paying those to spread a message using social media or through crafting a message to make it spread quickly.

A state may choose to conduct propaganda operations in the ways discussed above for two reasons. Firstly, it allows for a message to reach a large population if targeted in such a way, or, if it is chosen to, it could be used to target a particular section of the population. Secondly, operations like these, if conducted in a reasonable way, would allow a government to maintain plausible deniability. This is because it is very hard to prove whether or not an account has links to a government. Even when a particular person 'defects' for this kind of social media operation as was discussed with the case of Russia, it is still almost impossible to prove that a particular group is involved. What all this information clearly shows is that a number of countries are involved in this type of operation.

It is not just through messaging platforms such as *Twitter* that states have developed social media propaganda operations; they are also using video platforms such as *YouTube*. One example of such a campaign was conducted by the US State Department under the organisation that is now called the Center for Global Engagement that have conducted propaganda campaigns against IS. In this campaign, the State Department created a least one propaganda video that was designed to be similar in its composition to the propaganda videos of IS. This video was published on 22 August 2014. In this video, titled 'Welcome to the 'Islamic State' land' it has a caption that states 'where you can learn useful new skills for the Ummah!'[49] It then

[47] Edward Snowden Document, GCHQ, 'Full Spectrum Cyber Effects SIGINT Development as an Enabler for GCHQ's "Effects" Mission', ca.2010, p. 9, Snowden Surveillance Archive.
[48] Ibid., p.13
[49] US Department of State, 'Welcome to the "Islamic State" land', https://www.youtube.com/watch?v=-

goes to show that these new skills are 'blowing up mosques, crucifying and executing Muslims'.[50] It then has images from other videos that have been shown by the IS in an attempt to show the actions of IS against the Muslim world. The video has been seen as of the, 8 of March 2016 891,426 times. It finishes with the seal of the Department of State. It could be argued that this type of operation may well have been more effective had it not included the seal of the State Department. This is because then it has become clear that the US had made the video rather than leaving the organisation behind the video unknown. Nevertheless, it was argued that this operation and other operations conducted by the Center for Global Engagement had caused a 'significant irritation to its target'.[51] However, it must be noted that this campaign did receive a lot of criticisms and the coordinator, Alberto Fernandez, was replaced in February 2015, although it was unclear if Fernandez was removed because of this video campaign. Furthermore, campaigns like this could often be hard to judge in terms of successes. This is, as was noted in an interview with *The Washington Post*, unless some person says that they had planned to join IS until they saw this video and that this video made them stop, then it will never be clear whether it was a success.[52] Nevertheless, even if this video did not stop any recruits from joining IS, it does show ways in which cyber offensive operations can be conducted where states can create videos that are designed to promote a particular message. Furthermore, as was stated above, GCHQ developed a tool that allows for a video popularity to artificially increase.[53] This could then make those who are thinking of joining a terrorist organisation believe that the videos were more popular, and as such that it would be wrong to join a terrorist organisation. In this way, it could be argued that the hope would be that other organisations like news organisations think that a video is popular and then discuss and show the video. This would then mean that the video was reaching an even wider audience.

It appears that the use of videos to target people who are on the verge of joining a terrorist organisation was adapted and expanded by the US government.

---

wmdEFvsY0E&oref=https%3A%2F%2Fwww.youtube.com%2Fwatch%3Fv%3D-wmdEFvsY0E&has_verified=1, last accessed on 08.03.2016.

[50] Ibid.

[51] Greg Miller and Scott Higham, 'In a propaganda war, U.S. tried to play by the enemy's rules; Confronting The 'Caliphate'' ,*The Washington Post Blogs*, first published on 08.05.2015 accessed via Nexis Business and News

[52] Ibid.

[53] Edward Snowden Document, GCHQ, 'JTRIG Tools and Techniques', 05.07.2012, p. 5, Snowden Surveillance Archive.

This is because, it was argued, the Center would not, as was the case in the 'Welcome to the 'Islamic State' land', finish with the seal of the State Department. The Center will instead focus on expanding the videos that others have created rather than focusing on producing or using the material from the US government. This means that instead of videos if they were posted online on sites such as *YouTube* being clearly from the US, they could have come from anywhere. This has led to the idea that the group will act through providing invisible financial support to those who are making videos that work as propaganda against terrorist groups. To help conduct this type of operation, it was argued that the Center for Global Engagement would 'also employ data analysts who will work with private industry partners to sift through the public information any user leaves on social media, to determine who might be leaning toward radicalism and message them directly'.[54] This would allow the campaign to be more effective in its targeting. To support the idea of using videos as a way for governments to be involved in the propaganda campaign against terrorist organisations, it has been argued by the *Facebook* spokesperson Jodi Seth that videos are much more successful in conducting propaganda campaign than messages.[55] This goes on to show that states can use cyber offensive operations to target terrorist organisations by conducting propaganda campaigns.

It also appears that the US changed the way in which they conducted propaganda campaigns against terrorist organisations and caused it to become more covert. This can be seen in the fact that the Center for Global Engagement changed their strategy from conducting a direct propaganda campaign, in which they were the organisation that was creating and controlling the messages, to instead looking to 'amplify' the messages that others were spreading. The premise appeared to be that the Center for Global Engagement would be used to provide covert financial and technical support to those who are making videos and help these to spread their messages online.[56] This could have a higher impact, as it could be used to strengthen the image of those people who were viewed to be more influential to the would-be recruits. These could be those who were defectors from a terrorist organisation and

[54] Kimberly Dozier, 'Anti-ISIS-Propaganda Czar's Ninja War Plan: We Were Never Here', *The Daily Beast*, first published on 15.03.16, http://www.thedailybeast.com/articles/2016/03/15/obama-s-new-anti-isis-czar-wants-to-use-algorithms-to-target-jihadis.html, last accessed on 23.03.2016.
[55] Ibid.
[56] Ibid.

the Center for Global Engagement were to be used to spread the message further, albeit covertly.

Although the example that was discussed above shows that states are using propaganda cyber offensive operations via videos against terrorist organisations, it is clear that states have also used these types of operations against each other. It was argued that there is evidence that Russia has made use of *YouTube* to spread propaganda. This can be seen in the fact that NATO stated that there was clear evidence that Russia has used *YouTube* as a platform to spread videos that were being used to create a negative image of Latvia.[57] Further, it was noted by the Joint assessment of Russian involvement in the US Elections that 'according to R[ussia] T[oday] [RT is a Russian state run media organisation] management, RT's website receives at least 500,000 unique viewers every day.[58] Further, it was noted that RT has one of the highest number of subscribers to its *YouTube* channel.[59] Finally, it can be seen that due to the fact that the Center for Global Engagement has, due to the National Defense Authorisation Act (NDAA) 2017, been given an active role in combatting foreign state propaganda. This can be seen in that it was stated in the Act that the Center would

> Identify current and emerging trends in foreign propaganda and disinformation in order to coordinate and shape the development of tactics, techniques, and procedures to expose and refute foreign misinformation and disinformation and proactively promote fact-based narratives and policies to audiences outside the United States.[60]

Although it applies to any country, it does seem that, based on the political climate at the time, the immediate future of these activities would be directed towards the Russian state. Because of the skills that the Center for Global Engagement has, and the fact that Russia was conducting operations on *YouTube*, it seems reasonable to infer that there will be operations directed towards video platforms such as *YouTube*. In these ways, online videos have been one of the ways that states have been conducting propaganda cyber offensive operations.

---

[57] NATO STRATCOM, 'Internet Trolling As A Tool Of Hybrid Warfare: The Case Of Latvia', no date given, p. 42.
[58] Office of the Director of National Intelligence, 'Intelligence Community Assessment Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution' 6 January 2017, p. 10.
[59] Ibid., p. 10.
[60] US Government, 'National Defense Authorization Act For Fiscal Year 2017', Conference Report To Accompany S. 2943 30 November 2016 Section 1278 B(4)

Another way that states have been using cyber offensive operations for propaganda via social media is the targeting of news forums. The targeting of news forums and blogs gives states the ability to conduct propaganda campaigns. The purpose of this type of operation, as with social media, is to spread a particular message. Marat Burkhard provides evidence of this type of operation. He argued that he was used by the Russian government to promote a story once it had been published on a news outlet.[61] He states that to achieve this, Russia would promote a message on forums. He states to do this Russia would have a team of people: one would play a person who disagrees with a message a country is trying to promote and others would play the people who would promote the message.[62] This further allowed them to control a conversation. By controlling a conversation, it allowed them to win an argument and further promote a particular propaganda message.

GCHQ have demonstrated a willingness to conduct very similar operations. They have argued that they have considered setting up a blog that is from a 'victim'.[63] In this type of operation, a state would look to create a blog that appears to have been a victim of the terrorist organisation that is being targeted and then use this to show the effects that this terrorist organisation was having. This was to try and deter people from supporting this organisation. It could also come from someone who has, in some way, been affected by a state.[64] Although in the document it indicates that it has been used against countries, it is equally possible that it could be used against terrorist organisations in the sense that it would provide a way to show a particular point. For example, it could be done through purporting to be someone whose family has been killed to argue that the terrorist organisation is barbaric. In addition to claiming to be a victim of a terrorist organisation, it could equally be used in a way in which a profile could be set up to look like a former terrorist who had seen the error of their ways, who has turned away from the terrorist organisation. The types of propaganda operation, it could be argued, would be likely to be more effective in the sense that, if it appears to come from a government, then people may well question the information that is being sent.

---

[61] Paul Gallagher, 'Revealed: Putin's army of pro-Kremlin bloggers' *The Independent* first published on 27.03.2015'http://www.independent.co.uk/news/world/europe/revealed-putins-army-of-prokremlin-bloggers-10138893.html, last accessed on 28.03.2013.
[62] Ibid.
[63] Edward Snowden Document, GCHQ, 'SigDev Conference 2012 Cyber Integration: The Art of the Possible' with added notes by NBC News, ca. 2012, p. 8, Snowden Surveillance Archive.
[64] Ibid.

Not only is there an ability for governments to use human directed social media cyber offensive operations but it has become clear that there are a number of examples of governments developing operations that the author has termed technical led social media operations. The purpose of these types of operations is to create a system where a message is spread rapidly with little involvement from humans beyond creating the message in the first place. One way of conducting this form of operation is through the development of tools that allows one person to control a large number of social media accounts and spread messages across all of their accounts. It has been argued that the US government has developed or was developing tools to use social media for a propaganda campaign. In 2011 a company in the US was contracted to develop a tool that would be used, at the time, by US Central Command (CENTCOM) that oversees US armed operations in the Middle East and Central Asia. The company developed what is described as an 'online persona management service' that allows one US serviceman or woman to control up to 10 separate identities based all over the world.[65] This software was part of Operation Earnest Voice that was aimed at conducting a number of propaganda campaigns against a number of Middle Eastern countries.[66] This software, it was argued, allowed the US military to secretly manipulate social media sites by using fake online personas to influence Internet conversations and spread pro-American propaganda.[67] What this software allows is a single operator to have the ability to appear to be a number of different 'people'. This then allows the operator to spread a message with the appearance that the message had come from all over the world. This would allow a particular piece of propaganda material to be spread.[68] Further, this kind of software allows states to produce messages that cannot be traced to them. In the operation discussed above, each online identity had a complete history and background to make it difficult, if not impossible, for it to be traced back to a particular operation.[69] Amble argued that because the operation would not target *Facebook* or *Twitter*. This was deemed to be an issue because of the popularity of these websites.[70] Nevertheless, it is clear that this type of

[65] Nick Fielding and Ian Cobain, 'Revealed: US spy operation that manipulates social media', *The Guardian*, first published on 17.03.2011, http://www.theguardian.com/technology/2011/mar/17/us-spy-operation-social-networks, last accessed on 17.04.2015.
[66] Ibid.
[67] Ibid.
[68] Ibid.
[69] Ibid.
[70] Amble, 'Combating Terrorism in the New Media Environment', 346.

operation does allow for messages to be spread via social media. This allows states to spread propaganda.

GCHQ has also developed tools that could be used for the spreading of messages using social media. The first of these was a tool called CLEAN SWEEP. This tool had two abilities (the other will be discussed below). The first ability is that CLEAN SWEEP was able to spread a message via *Facebook* to whole countries.[71] This ability, they argued, was ready for use. This would allow for a propaganda message to spread rapidly. A further tool that was developed was called GESTATOR. This had the ability, it was argued, to amplify a message or possibly a comment that was connected to videos and seems to have been created for platforms similar to *YouTube*.[72] The use of both of these tools would mean that a message could be spread rapidly allowing it to reach a large number of people. In these ways, it is clear that a large amount of research has gone into the development of technical tools to spread propaganda.

GCHQ developed had the ability to increase web traffic through the use of a tool termed GATEWAY.[73] The ability of this tool was that it allowed GCHQ to artificially increase the numbers of visitors to a website. If this tool were to be used in conjunction with the spreading of false information through a blog or a forum, it would allow them to increase the power of the message and allow it to appear to be true.[74] There are two other tools that GCHQ have developed to further the goal of spreading propaganda. The first is SLIPSTREAM, this has the same ability as GATEWAY. GCHQ also developed SKYSCRAPER, this had the ability to spread multimedia information around and promote it.[75] Furthermore, as with the use of fake profiles for social media that both the British and the US have clearly developed, it means that it could be used for forums and news websites. In all of these ways, it is clear that many governments have developed tools that allow them to conduct cyber offensive operations for a propaganda purpose.

In addition to using technology to help spread a message, states also have the tools to create the messages without the need of humans. On social media platforms

[71] Edward Snowden Document, GCHQ, 'JTRIG Tools and Techniques', 05.07.2012, p. 5, Snowden Surveillance Archive.
[72] Ibid., p. 5.
[73] Ibid., p. 5
[74] Ibid., p. 5
[75] Ibid., p. 6

such as *Twitter*, this has been achieved through the creation of bots that create their own message and then spread them. These systems have been preprogramed to send out information when particular criteria are met, or just at random times but with information that has been preselected. In this, the actual message does not need to have any other human interaction beyond the initial programming. The benefit of this is that these systems can spread information a lot more quickly. However, it could be that they will be less able to craft the message effectively. Nevertheless, it was argued that the French intelligence agencies were worried during the French elections that covert social media propaganda would become a major issue.[76] It is unclear if there was a large number of *Twitter* bots spreading messages and, if so, how effective they were, but what is clear is that states will likely continue to use these in the future.

One reason for the development of social media operations in all their forms that have been discussed throughout this section is that they, as GCHQ argued, allow for an influence on people which is far greater than that of traditional forms of propaganda campaigns like the radio and television. If this is the case, then it would mean that a propaganda campaign designed to use social media would possibly allow it to target larger number of systems, it could also control a conversation on social media.

The other benefit of using social media to conduct propaganda campaigns is that these types of operations can be picked up by traditional media organisations who then publish a story based on this information. This allows for the information to spread even further. An example of this is in 2017 when Fox News (a US news organisation) and President Donald J. Trump stated that GCHQ had been used to spy on Trump when he was campaigning to become president. The former director of GCHQ Robert Hannigan said that in January and February GCHQ had come across blogs in Macedonian that had suggested that GCHQ had been tasked by President Obama to spy on Donald Trump. This story about GCHQ spying on Trump was then picked up by Alt Right websites. Finally, it was then picked up further and spread on *Fox News* and entered the mainstream news.[77] Hannigan did point out that GCHQ did

[76] Emily Tamkin, 'French Intelligence Agency Braces for Russian Bots to Back Le Pen', *Foreign Policy* first published, 08.02.2017 https://foreignpolicy.com/2017/02/08/french-intelligence-agency-braces-for-russian-bots-to-back-le-pen/, last accessed 08.02.2017.
[77] Robert Hannigan, 'Mission Possible 2017', *Aspen Security Forum* Moderator David Ignatius Speakers Admiral Mike Rogers Director of the NSA and US Cyber Command and former head of GCHQ Robert Hannigan. Speaking 07:50-8:36

not trace this story to see if the Russians, in a cyber offensive operation, planted the information. By propaganda being picked up by news agencies that had originally been placed on social media and then stating it as news, it is possible that people are more likely to believe the story. This clearly shows one of the benefits of using cyber offensive operations for propaganda, as there is a chance that the story can spread and be picked up by traditional mass media and spread even more.

However, there are a number of issues with conducting a cyber offensive campaign that is designed for propaganda. The first is making sure that the message reaches the target audience. Although this is always an issue with propaganda campaigns, it could be more of a challenge in an online setting. The Internet is vast, meaning that people will often choose what they want to look at. In terms of social media, it means that the targeting of messaging must take place. This though presents no more of a problem than traditional forms of propaganda that have all been used in the past. Because both GCHQ and US CENTCOM are using this type of operation, it clearly shows that governments are seeing that there must be some benefit. Furthermore, the Defense Advanced Research Projects Agency (DARPA) that works for the US Department of Defense stated that they place contracts for the Social Media in Strategic Communication (SMISC) program. The purpose of this programme was to develop tools that would allow groups to identify these types of operations and counter them.[78] This must mean that, in terms of the social media forms of propaganda, it must be seen as having either a negative or positive effect for the Department of Defense to want to develop this software. This can be seen in the fact that GCHQ argued that both types of operations provide the ability to use these operations for 'personal' style operations, target 'community of interest' or a 'global audience'.[79] It can, therefore, be argued that this is one of the ways that government have developed the use of cyber offensive operations.

It also appears that a further area in which states have engaged in propaganda campaigns has been directed against computer games. It was noted in a document created by a contractor working for the NSA, that they were 'establishing an in-game presence allows for virtual interfacing, information exchanges, and developing

[78] DARPA, 'Social Media in Strategic Communication (Smisc)' http://www.darpa.mil/Our_Work/I2O/Programs/Social_Media_in_Strategic_Communication_(SMISC).aspx, last assess on 28.05.2015.
[79] Edward Snowden Document, GCHQ, 'The Art of Deception: Training For a New Generation of Online Covert Operations', no date given, p. 19, Snowden Surveillance Archive.

influential relationships with both adversaries and allies. In-game interaction also can help shape real-life attitudes and perceptions'. [80] This would then allow for governments to use online games to spread propaganda about a terrorist organisation. It has been argued that the use of such operations can change real world perceptions.[81] GCHQ had developed a tool that would work inside computer games or online games. They had developed a tool called GLITTERBALL, which, according to them, had a use for 'Online gaming capabilities for sensitive operations', and that it was 'currently Second Life'.[82] This means that it has been used in the online game Second Life.[83] This then clearly shows that states have been looking at new ways in which they can use cyber effects in a propaganda campaign against a terrorist organisation.

A further way that states may, in the future, be able to use cyber offensive operations to spread propaganda against other states or organisations is through using programs that are embedded into popular websites. On the 30 of March 2016, Microsoft announced that it had developed a programme that could interact with people on the service *Skype*. This is because the programme will be used to represent businesses on *Skype* and sell products and services. Although the system is designed to work for companies and to promote a business, it could be used to examine a conversation between friends about, for example, a planned holiday and then the programme would come in and promote a travel agency or a trip website it could be used for state propaganda.[84] This is because it would be able to identify particular features of conversations and respond to them. Therefore, if a conversation took place and a person began talking about going to Syria, the programme could respond by sending out anti-terrorism propaganda. However, it must be noted that programs like this have had a troubled past. This can be seen in the fact that Microsoft had to take offline a system like this that worked on *Twitter* after it became too racist.[85] However, although the system at the time of writing this has not been perfected, it could, in the

[80] Edward Snowden Document, SAIC 'Games: A look at Emerging Treads, Uses, Threats and Opportunities in Influence Activities', n.d, p. 62, Edward Snowden.com.
[81] Ibid.,
[82] Edward Snowden Document, GCHQ, 'JTRIG Tools and Techniques', 05.07.2012, p. 5, Snowden Surveillance Archive.
[83] For more information on Second Life, see Kim Keeline, 'Second Life', in Thomas Riggs (ed), *St. James Encyclopedia of Popular Culture* Volume 4, Second Edition (Detroit: St. James Press, 2013), pp. 485-486.
[84] Chris Baraniuk, 'Build 2016: Microsoft proposes helper bot boom', *BBC News*, first published on 30.03.2016, http://www.bbc.co.uk/news/technology-35927651, last accessed on 06.04.2016.
[85] No author given, 'Microsoft 'deeply sorry' for racist and sexist tweets by AI chatbot' *The Guardian* first published on 26.03.2016, last accessed on 06.04.2016, accessed via Nexis Business and News.

future, be a useful system for propaganda operations. In addition, *Facebook* have announced that they will also be developing this technology.[86] Although these systems are still untested and are not yet operational, and even though there is no evidence that states have begun to look at using these systems, in this author's opinion it is likely that these systems, or systems that work on similar principles, could and will be used by states to conduct propaganda cyber offensive operations.

In all of the ways that have been discussed above, it is clear that states have a number of ways in which they can use cyber offensive operations to conduct propaganda campaigns. These systems can be used against both state and non-state actors.

Direct Counter Propaganda

Another area of cyber offensive operations is direct counter propaganda. Although all propaganda can work as counter propaganda, in that a state will combat the messages of another, direct counter propaganda operations are different. Direct counter propaganda, as this author has chosen to define these activities, are campaigns in which a state takes control of an adversary's system of conducting propaganda and then turns this against the adversary by changing the message. For example, a state could take control of a website and replace or in some other way change the information, or remove the information completely.

The reason for labelling these operations as direct counter propaganda and considering them as separate operations from that of propaganda is that, unlike propaganda, direct counter propaganda aims to take control of the target's own channels and use this to spread their own propaganda. This means that a state can target those who are looking at the other group's propaganda and change the message or the tone of the other group's messages.

An alleged example of this type of operation has been conducted against a terrorist organisation. This type of operation can be seen to have been used, allegedly, by the British Secret Intelligence Service (SIS) against Al Qaeda.[87] Known as

[86] David Lee, 'Facebook's next big thing: Bots for Messenger', *BBC News*, first published on 12.04.2016, http://www.bbc.co.uk/news/technology-36021889, last accessed on 13.04.2016.
[87] C.F. The Author has stated allegedly for a number of reasons. Firstly, the operation has not been confirmed to have taken place. Secondly, SIS has mainly been involved in Human intelligence and it

Operation CUPCAKE, this operation came about when it was discovered that there was an online English language Al Qaeda magazine that promoted the work of Al Qaeda and also provided support to Al Qaeda through providing instructions in constructing homemade bombs. In this operation, SIS replaced the link to how to make a homemade bomb with a link to a cupcake recipe. They also removed content that was created by Osama bin Laden, Ayman al-Zawahiri, and a piece about 'What to Expect in Jihad'.[88] In this way, the idea was to remove propaganda. Although the magazine was reissued without these changes later on and there have been further magazine articles from this source, it does show a way in which a state can use a cyber effects operation against terrorist organisations. This is because it can control what information is online. However, it could be argued that this type of operation in which a state apparently changes an online magazine would likely be limited. This is because it would be very clear when this took place. Nevertheless, this does not distract from the fact that this is a way in which states can look to conduct cyber offensive operations against terrorist organisations.

A further example of way that this type of operation could be conducted is through taking control of terrorist social media accounts. This can be seen in the fact Canada proposed a law in which they could take control of a terrorist recruiter's social media accounts and use these to then spread counter propaganda.[89] Although it is not clear if they have enacted this, it does show one of the ways that states could use cyber offensive operations against terrorist organisations for a direct counter propaganda campaign. However, there could be issues in this campaign. This is because if a state could gain control of a particular account, and then the messages suddenly changed then it could become very clear that someone had affected the system. This would mean that the organisation might stop using this system. Nevertheless, if there was a backstory to the change, as in the person had been in a particular country and involved in an operation and something forced them to change

---

would seem likely that this operation was actually conducted by GCHQ. Duncan Gardham, 'MI6 attacks al-Qaeda in 'Operation Cupcake', *The Daily Telegraph*, first published on 02.06.2011 last accessed on 23.03.2016, accessed via Nexis Business and News.

[88] Ibid.

[89] Lori Hinnant and Ken Dilanian, 'For US Allies, Paradigm Shift In Intelligence Collection', *Associated Press* first published on 20.05.2015, http://hosted.ap.org/dynamic/stories/E/EU_RETHINKING_INTEL?SITE=AP&SECTION=HOME&TEMPLATE=DEFAULT, last accessed on 21.05.2015.

their views, then it could be an effective form of activity. This then shows ways in which states can use cyber offensive operations against terrorist organisations.

It is not just terrorist organisations and the support websites that have been targeted by direct counter propaganda operations; states have targeted websites of news outlets that are spreading information which is propaganda and either spreading other information or stopping the website completely. One example of this was when the Syrian Electronic Army, which allegedly has links to the government of Syria, targeted *The Independent*. In this attack, the Syrian Electronic Army hacked into the website and posted a statement that read 'You've been hacked by the Syrian Electronic Army'.[90] In addition to *The Independent*, *The Chicago Tribune*, *CNBC*, *Forbes*, and *The Daily Telegraph* were also targeted.[91] This then shows that a state could either on their own or through groups that have links to it, target websites that they deem are spreading propaganda against them. This then shows that businesses are also being targeted in cyber offensive operations to spread counter propaganda.

In these ways, it is clear that one of the ways that states could use cyber offensive operations against both states and non-state actors is through direct counter propaganda operations where the adversary's own propaganda machinery is directed against themselves.

Comparison

It can clearly be seen that there is a large amount of overlap between propaganda that has been conducted in the past as covert action and cyber offensive operations. The first way that it can be seen that there is a direct connection between covert action and cyber offensive operations is that both have targeted states and non-state actors. This demonstrates that overall there is no real difference between these types of activities based on the groups that are targeted as part of the activities. Secondly, both types of activities have used white, grey, and black propaganda as part of their campaigns to target the adversary. States, whether using traditional covert action or cyber offensive operations to conduct propaganda, will use which ever form of information that they

[90] Andrew Griffin, 'Syrian Electronic Army hacks global websites including The Independent', *The Independent*, first published on 27.11.2014, http://www.independent.co.uk/life-style/gadgets-and-tech/news/syrian-electronic-army-hacks-global-websites-including-the-independent-9887176.html, last accessed on 18.03.2015.
[91] Ibid.

deem will be most effective to spread their message. They both use the same base to spread ideas in the hopes that they will force a change in their target so that a change of policy can be made.

Further, the same issues of reliability were shown to exist in both types of activity. This can be seen in the fact that the Official Committee of Communism Overseas noted that for their proposed propaganda activity to be successful they needed to find and establish a person who had credibility with the population. This issue can be seen to have been apparent to the Center for Global Engagement who changed their approach to the cyber offensive propaganda campaigns and focused on highlighting and enhancing those who they deemed to have creditability within the community that they were attempting to target.

Both types target the adversary in a number of different ways to be effective. In terms of traditional covert action, it was demonstrated that states have targeted particular reports to allow their message to be spread. Traditional covert action has, at times, even purchased entire news outlets to allow for the propaganda to spread effectively. Propaganda has used remote systems to allow for the propaganda to spread effectively with the use of radio propaganda. In terms of cyber offensive propaganda it is clear that states have attempted to use a multitude of platforms to allow for their propaganda campaigns to be effective. States have used social media to allow for propaganda to spread. They have targeted news outlets and other platforms. This then shows that both types of activities have targeted a number of different systems to allow for their operations to be effective. In this way it can be seen that the fact that cyber offensive operations have targeted different systems to that of propaganda as part of a covert action campaign does not make them new. It merely means that states have attempted to adapt to the world and using other methods to spread propaganda meaning the method is new rather than the activity itself.

A further comparison is that both types of activities have attempted to ensure that there message is spread further than the initial place that was targeted to make sure that the propaganda is effective. This was demonstrated with traditional propaganda in the fact that the Official Committee of Communism Overseas had hoped with the publishing of information on the Soviets use of forced labour would be picked up by other news organisations and that this would then spread the message even further. This hope can clearly still be present in the use of cyber offensive

operations in the fact that GCHQ had created tools that would allow for the particular message to appear to have been seen by more people. This, it could be argued, was in an attempt to make it look more popular. This would mean that others would pick up on that message and then it would be spread, as others believe that it is popular.

The only really 'new' type of activity that covert action that could be achieved through cyber means that this research has been able to find is direct counter propaganda. Although states have tried to disguise some of their propaganda efforts as if they are coming from the enemy, for example, via radio propaganda,[92] direct counter propaganda is different. Instead of conducting the propaganda campaign by trying to ghost a system, a term for radio propaganda in which a state broadcasts close to the same frequency of the target in the hope that people would accidently tune in, in direct counter propaganda a state will look to take control of a target's already established propaganda website or messaging forums. The state would then look to change the material, either subtly or obviously, the choice being based on what the state was looking to achieve. From this, the target would see the changed message and overall the propaganda could change their outlook, or it could be used to create some other form of panic within the organisation or group that a state is targeting.

Overall therefore, it must be concluded that there is no real difference between covert action and cyber offensive operations in terms of propaganda campaigns. The only real difference is that cyber offensive operations can target a larger number of people in a shorter amount of time. Both types of activities are conducted using a variety of activities and they will use true and falsehoods depending on what it is that they are trying to accomplish. This then shows that to a large extent there is nothing 'new' with cyber offensive operations and covert action in terms of the propaganda activity.

Conclusion

This chapter had a number of aims. Firstly, it aimed to demonstrate how states have in the past used propaganda as a form of activity as part of covert action to target other states. It has clearly demonstrated that states have used covert action to conduct a propaganda campaign in a number of ways. Firstly, they have attempted to recruit reports or news organisations to allow for a particular message to be spread. They

[92] Godson, *Dirty Tricks and Trump Cards*, p. 152.

have used radio to remotely spread messages, and they have at times even bought entire news organisations to allow for states to spread particular messages.

The second aim of this chapter was to highlight the ways that states have and could in the future use cyber offensive operations to spread propaganda. It has clearly demonstrated that states have attempted to use social media to spread propaganda. They have established different systems for this whether they use humans to conduct the operations or whether they are using technology to allow for a particular message to be spread. States have also targeted news organisations and forums for the campaigns to be successful.

This chapter did discover that a type of activity that has taken place as a form of cyber offensive operations is what this author had termed direct counter propaganda. This type of activity is where a state will take control of the system that one organisation is using to spread propaganda. This state would then take control of this system and use it against the group that created the system.

Most importantly, this chapter provided a comparison between traditional propaganda and cyber offensive operations that is aimed at conducting propaganda activities. It argued that, overall, it can be clearly argued that there is nothing particularly new about the use of cyber offensive operations and covert action in terms of the propaganda. Both types of activities have in the past targeted both state and non-state actors. Therefore, in terms of choice of target, it clearly demonstrated there was noting particularly new between the activities. Secondly, the information that is spread in both types of activities could be real or false or somewhere in between. This then shows that there is nothing particularly new between these types of activities. Both types of activities have attempted to use a number of different ways for the activities to be spread. This, therefore, should be seen merely as an evolution of an activity rather than a new activity overall.

CHAPTER THREE

Covert action and Cyber Offensive Operations: A Comparison between Political Activities.

This chapter will compare the activities of traditional covert action that has been deemed to be political to those of cyber offensive operations that can also be seen to be political in nature. This chapter will develop the argument that overall it can be seen that a direct comparison between covert action and cyber offensive operations can be drawn. This chapter will argue that overall the use of cyber offensive operations for political operations in nothing new and that they can be seen to be at most an evolution of the activities that have already taken place in the past.

To demonstrate this argument this chapter will firstly highlight the ways that covert action has in been used in the past to target other states and non-state actors. This will show that there have been a number of different ways that states have used covert action to conduct political activities. It will follow that argument of Kahn that actions that states take can be seen to follow a hierarchy of aggressiveness in terms of the operations.

This chapter will also demonstrate the ways that states have used cyber offensive operations to conduct operations that can be seen to be political. It will argue that there are six ways that states have in the past attempted to use cyber offensive operations in the past to conduct political cyber offensive operations. Firstly, defacement operations: states have defaced a government or political website. Secondly, stopping government websites from working; this is where a state will target the websites of other states to stop them from working. Another form of cyber offensive operations that are political is a publication. This is where states have published information that is damaging to another state. Fourthly, target and relational; this is where a state will conduct an operation in such a way that people are acutely aware who has conducted the operation but cannot prove it. This is to send a clear political message. A fifth form of activity is a resentment campaign. This is where a state will use cyber offensive operations to target a particular group or groups within a state or non-state actor to create resentment within the target. Finally, voting systems. This type of operation is where a state will attempt to affect the voting

systems within a state. This final part of this subchapter will examine complete cyber offensive operations that can be seen to have taken place. It will focus on the Russian campaigns during the 2016 US presidential elections, although it will look at some wider campaigns that can be seen to have taken place. The reason that this is so important to do is that these complete operations clearly demonstrate the use of cyber offensive operations for political purposes and in terms of the US elections have and continue to have political ramifications.

Traditional Covert Action: Political Activities

Political as a form of covert action covers a very broad range of activities. The aim of these activities is to affect the power and policies of another country.[1] Political operations do not always need to try and defeat a hostile power either in an election or by subverting a government and causing them to collapse. A political covert action campaign can also be aimed to change a policy of a particular state or group. There are many ways that political covert action can take place.

One way that political covert action can take place is by one state supporting a political party that is opposed to the person or government that this state wants to affect. An example of this type of operation was when the CIA, in 1964, provided around 2.6 million dollars to help a Christian Democrat candidate to try and stop the Marxist candidate from gaining power in Chile.[2] This activity should be seen as political due to the fact that the money was used to gain a political objective rather than an economic activity that will be discussed below. This was also supported by providing funds to at least two other political groups in Chile in the 1964 election. This was in the hopes that by helping to other political groups, it would cause the domestic political votes in Chile to be divided so that Salvador Allende would not win in the election.[3] The aim of these operations is to allow for the organisations to which the money is being supplied to make sure that they can still function.

This type of activity can be effective for one state to use against another state when a particular group seems to be popular with the people of the target state. This is because the state that is conducting the covert action is able to stop them from

[1] Rositzke, *The CIA's Secret Operations*, p. 185.
[2] United States, Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, 'Church Committee Covert Action in Chile 1963-1973 Staff report of the select committee to study governmental operations with respect to intelligence activities', p. 9
[3] Ibid., p. 9

functioning by making it difficult for them to win in an election. In addition, it can also be of use when it appears that the group that is the target of the state that is instigating the covert action is competing against a different group that is being financially supported by another state.

This was clearly evident to be as an effective tool during late 1940s when both America and Britain were fighting to keep many parts of Western Europe from moving towards communism and the Soviet Union was aiming to try and turn parts of Western Europe towards communism. One of the main examples of this type of operation took place in Italy in 1948,where the US secretly gave funds to political groups as well as their political leaders in the hopes that the money would help them defeat the Communist Party in Italy.[4] It has been argued that the supply of money to these groups continued at least until 1968 and amounted to millions of dollars a year.[5] This type of activity was also used in Nicaragua. It was argued that the US should provide financial aid to groups that opposed the Nicaraguan government because this would allow them a position of strength in which they could deal with the government. It was felt that providing money would allow them to do this.[6]

A further way that political activities can take place is through a personal contact. This can be seen in the case of British involvement in the US during the build-up and during the start of the Second World War. This organisation, because of the relationship that was built up by Stevenson, was able to influence the way in which the US government acted towards the Germans. For example, the BSC was able to make connections to Robert Sherwood, that, it was argued, worked with President Franklin Roosevelt in the creation of Foreign Policy speeches allowing the British to 'add its point of view'.[7] It was argued that this was a political operation that allowed Stevenson to both directly and indirectly affect US public opinion and possibly even the President of the United States himself.[8] It was argued that all of this was used to move the US away from their policy of isolationism.[9] The use of this type

[4] Rositzke, *The CIA's Secret Operations*, p. 187.
[5] Ibid., p. 187.
[6] Brown University, Public Diplomacy Office Review, 'Scope of CIA Activities under the Nicaragua finding September 19, 1983',
https://www.brown.edu/Research/Understanding_the_Iran_Contra_Affair/documents.php, p. 1.
[7] West (ed), *British Security Coordination*, p. 16f
[8] West (ed), *British Security Coordination*, p. 16f
[9] William J. Daugherty, 'Covert Action: Strengths and Weaknesses', in Loch. K. Johnson (ed), *The Oxford Handbook of National Security Intelligence* (Oxford: Oxford University Press, 2010), p. 611

of operation is more than just secret diplomacy when it is conducted by non-ambassadors and conducted by intelligence operatives. This is because of the fact that the aims are often such that those in each government do not want the information to be acknowledged. In addition, it moves beyond secret intelligence liaison because the aim is to achieve a change of or keeping a political policy rather than simply to gather intelligence.

A further way in which political covert action has taken place is through agents of influence. An agent of influence is the use of a private individual who is not an officer of an intelligence service but who works in a foreign country. They are used by the government who is looking to conduct the covert action when needed, to advance the aims of the covert action government in the foreign government. The idea of an agent of influence is over time to get into a position of power within or with contact with foreign government personnel to allow a government to advance its own goals. This type of operation can and usually does take a long period of time to achieve because they must wait for the agent to get into a position of power. In addition, both the British and the US looked to use this as a way to get the Shah of Iran in 1953 into a heightened position of power within his own country. The plan was to use the Shah's twin sister Princess Ashraf, who they referred to as 'forceful and scheming' to help them to convince the Shah to follow the policy of removing Mossadeq. It was not just the western powers that have used this form of covert action. It was argued that the Soviet Union were able to use this type of operation in a number of cases where, even if they would not build up an agent over time, they would bribe someone to represent Soviet interests in foreign governments. It has been alleged that the Soviet Union were able to get a leading member of Mussolini's cabinet to work for them in this way.[10]

It has been argued that the US government were very good at conducting these types of operations in the late 1940s and 1950s. This is because, after the Second World War, the US took an active involvement in the recruitment and advancement of people inside Europe and helped them to develop the ideas of what they wanted to do with their country. This type of operation is likely to take a long time to develop because the agent is aimed at helping their agents to become effective.

[10] Alexander Orlov, 'The Theory And Practice Of Soviet Intelligence', *Studies in Intelligence*, 7:2, (1963), https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol7no2/html/v07i2a05p_0001.htm,

A further type of political covert action can be conducted through providing assistance in running campaigns, in addition to helping to provide funds. This was particularly clear in the case of Chile in which a joint team of people from the State Department, the White House, and the CIA were used to provide advice to the Christian Democrat groups within Chile on how best to win elections.[11] This help included advice on how to poll and how to increase the level of people to voting by providing help with voter registration.[12] These activities were clearly being used by the US to allow them to influence the outcome of elections, thus being a political covert action campaign.

The leaking of information is another way in which covert action can take place. This can be done through intelligence agencies or it can even work through diplomats who have contacts in a particular area in terms of work. As such it can allow for one state to leak information that another state does not want their population to know or a select group of their population to see, or even leaking information about one state to the population of another state to create discontent within this state. The leaking of information should be placed higher on the ladder than propaganda. This is because the level of violence of getting information and leaking is higher than that of simple propaganda. This is because these types of operations will usually have documents to provide evidence of a particular point that a state is looking to put forward. By providing evidence of an internal view of a political candidate it could force that political candidate to change their policy due to it being unfavourable or it could force this person to withdraw completely from an election allowing the covert action instigators to have the candidate they want elected. Although there are no clear examples of a covert action campaigns that have used this method, it is not hard to imagine that it has formed at least part of a covert action programmes that have been conducted in the past.

In addition to leaking information, states have also conducted campaigns in which they spread false information by providing fake documents or evidence against a particular state or group that they are looking create issues with. There are two ways

[11] United States, Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, 'Church Committee Covert Action in Chile 1963-1973 Staff report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities', p. 9.
[12] United States, Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, 'Church Committee Covert Action in Chile 1963-1973 Staff report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities', p. 9.

in which this is different from a propaganda campaign. Firstly, it is usually supported by supplying 'evidence' of a particular policy. For example, when the Soviet Union had looked to try and get the Indian government to move away from the US and become friendlier to the Soviet Union. They produced, in 1987, a forged document that 'showed' that the CIA had been looking to overthrow the Prime Minister Rajiv Gandhi.[13] This type of operation is different from propaganda. This is because the state that is conducting the activity, is hoping that the false information is believed by the people who are position of authority rather than the general population itself. By getting the leaders, or at least those with sufficient power, to believe the information would produce a favourable action to help the instigators of the covert action.

This form of operation can be seen to have taken place, when the British attempted to get the Soviet Union to remove and destroy an organisation of their government. The British attempted this under a codenamed Operations HOUSE PARTY. This operation had a number of objectives. However, one plan was to target the effectiveness of the Soviet Union's internal security agency, the MVD and, hopefully, make the Soviet leadership think the MVD was working against the Soviet Union. It was argued that this organisation was chosen because this was how the Soviets maintained a grip on the regime and the Soviet Union's effectiveness rested 'ultimately on the efficiency and reliability of the MVD, without which it could not function'.[14] This plan was to conduct framing operations by planting evidence that indicated that members of the Soviet government or the MVD were working for the British. The aim of the framing operation was that it would create a great deal of uncertainty about the reliability of the government machinery and the MVD.[15] The British wanted to force 'the Russians would react favourably if we could persuade them that there was dissention within their ranks. This might be in the MVD or in a strong underground anti-Kremlin resistance group'.[16] There were two plans that evolved from this. One plan was directed against a member of the Russian administration. By conducting such a program, the British would have affected the relationship between the Intelligence service of the Soviet Union and their leadership. Due to the fact that the Soviet Union was totalitarian, it was likely that these

[13] Andrew and Mitrokhin, *The Mitrokhin Archive II*, p. 339.
[14] TNA, DEFE 28/43, 'Future Deception Policy For Adverting War' Policy for Deception Note By Controlling Officer , General Factors affecting Deception in Peace, 09.08.50, p. 3.
[15] Ibid p. 4
[16] Ibid p. 1

intelligence officers could have been killed because of this information. In addition, these operations could have destabilised the Soviet Union.

The most extreme form of political covert action is a coup d'état. The use of a coup d'état is that one state will force a change of government from another state. One example of this operation was undertaken by a joint US British operation to remove the Premier of Iran Mossadeq in 1953. It was felt that if the US and the UK did not conduct an operation to remove Mossadeq, then Iran would economically collapse, causing Iran to fall into the orbit of the Soviet Union.[17] They were successful in causing the coup and getting the Shah of Iran to have complete control. The coup used the same methods as those discussed above; it used propaganda to turn the people of Iran against Mossadeq.[18] It also used agents to cultivate the Shah of Iran, and the British and the US used Princess of Iran Ashraf to work as an agent of influence on the Shah.[19] In these ways, the coup worked in overthrowing Mossadeq and allowed Iran to come into the Western sphere of influence over twenty years.

There are, as was shown above, many different ways that states can conduct political covert action. Political covert action, in whatever form it takes, aims to 'try to manipulate policies by influencing popular thinking about an issue or it can focus on a single key official, or on a few key individuals'.[20] The key point that joins these actions together is that the actions are aimed, as Rositzke states, with attempts to undermine the power and policies of a foreign power.[21]

Cyber Offensive Operations Political Operations

It can be seen that there is ability for cyber offensive operations to be used to conduct a campaign that is political in nature. This type of activity can take place in a number of ways. There are several different ways that states have used political operations to target both state actors and non-state actors. These included: defacement; stopping websites from working; attacking particular organisations to spread a message; publication operations; resentment campaigns; and possibly, conducting a cyber offensive operation to affect voting systems.

---

[17] The National Security Archive, CIA, Clandestine Services History, Dr. Donald N. Wilber, *Overthrow of Premier Mossadeq of Iran: November 1952 - August 1953*, March 1954, Appendix B, p. 1.
[18] for a full account of this operation and how it was conducted see Ibid., Chapter II and III.
[19] Aldrich, *The Hidden Hand*, p. 473.
[20] Gallo, 'Covert Action', 355.
[21] Rositzke, *The CIA's Secret Operations*, p. 185.

There are operations that have, allegedly, taken place but it is not clear how they were conducted. In a GCHQ document that was leaked by Snowden, it appears that GCHQ have completed political cyber offensive operations against at least two states. Firstly, it appears that a GCHQ operation was used to discredit the regime in Zimbabwe.[22] This is clearly a use of offensive cyber capabilities for a political purpose even if it is not clear how it was conducted. The document indicates that they may have targeted the population of Iran as well.[23] Although there are no clear indications on how these campaigns were conducted, there have been a number of examples of political cyber offensive operations that allow this researcher to understand the types of political cyber offensive operations.

Defacement

One way that cyber offensive operations have been used for a political operation is through the defacement of political websites. The purpose of this type of operation is to target a government system and change a picture or text on a website so it promotes a particular message. This type of operation has been used in several cases. One example of this type of operation was conducted by what appeared to be a group that had links to the North Korean government. Several websites linked to the South Korean government were targeted and banners were placed on the websites that read 'Long live General Kim Jong-un, president of reunification!'[24] A similar attack happened in 2008 in the Republic of Georgia. In this case a picture of the President of Georgia was changed to make him appear to be linked to Adolf Hitler.[25] The purpose of these types of operations are heavily interlinked with that of propaganda and direct counter propaganda campaigns. However, instead of simply spreading a message, they look to change something in a very public way. By changing a picture on a government website, the operation moves beyond a simple propaganda campaign as the group or government is directly challenging the control of a state, even if it is only through a website. Nevertheless, this type of operation is likely to have very little

[22] Edward Snowden Document, GCHQ, 'Behavioural Science Support for JTRIG's (Joint Threat Research and Intelligence Group's) Effects and Online HUMINT Operations' 10.03.2011, Snowden Surveillance Archive.
[23] Ibid.
[24] Ju-Min Park and James Pearson, 'North Korea's cyber spies exposed: Inside the secretive cyber-warfare cell Bureau 121', *Independent*, first published on 05.12.2014, http://www.independent.co.uk/news/world/asia/north-koreas-cyber-spies-exposed-inside-the-secretive-cyberwarfare-cell-bureau-121-9907161.html, last accessed on 05.12.2014.
[25] Clarke and Knake, *Cyber War*.

actual effect in terms of what people think. This is because it seems unlikely that someone's perception of a person or government will change dramatically, or even slightly, by stating a message or changing a picture on a website.

However, although the spreading of the direct message is unlikely to achieve a great deal in terms of changing a population's already held views, there are other reasons to conduct these operations. Firstly, this could force a government to shut down access to a website as they try to take down the message and improve the security of the website. Secondly, this type of operation creates publicity. This means that if it is connected with a political issue, this type of operation could be seen as something akin to warning shot or even work as a call to arms for protesters and force a government to question whether their proposed cause of action is worthwhile. Finally, it could also raise questions about security and how a government is protecting its citizens. What is clear though, is that this type of operation has been conducted and it is a way in which states are using their offensive cyber powers.

Stopping websites from working

A denial of service attack aims to stop government websites from working. These types of operations have been conducted either through the use of a DoS attack or a DDoS attack. The target website is flooded with so many requests to join that it cannot cope and shuts down. There are several ways that techniques like this can be used. But the purpose here is to discuss how tools like this can be used to achieve a political purpose. What causes these types of operations to be political in nature is that they target government websites and stop them from functioning so that a population of a given country cannot access them.

There have been several cases where this type of operation has taken place. For example, in 2007 a number of Estonian governmental websites were stopped from working using this type of operation. This included the Foreign Ministry and other government websites as well as the targeting of the political parties in Estonia.[26] Stopping access to government websites may cause people to question the government. It also means that a state affects the ability of another state to function because their systems which are connected to the website will be shut down. This

[26] Ian Traynor, 'Russia accused of unleashing cyberwar to disable Estonia', *The Guardian*, first published 17.05.2007, http://www.theguardian.com/world/2007/may/17/topstories3.russia, last accessed on 13.02.2015.

means that, with this tool, sharing of information within government can be stopped to achieve an objective. In these ways, it is clear that cyber offensive operations have been used and can be used to stop a government from working.

It is clear that it is not just government websites that have been targeted to stop them from working but non-state actors have also been targeted in very similar ways. This may even in fact have a greater visual impact on a larger proportion of a population as there are many sites that people visit on a day-to-day basis. This type of attack can be seen to have taken place several times. One example was the attack by the Syrian Electronic Army which has links to the Syrian government under President Bashir al-Assad. They targeted *eBay* and *PayPal* and stopped some people being able to access either service. In addition, the Syrian Electronic Army posted messages via their *Twitter* feed that said, 'for denying Syrian citizens the ability to purchase online products, Paypal [sic] was hacked by SEA' and 'if your Paypal [sic] is down for a few minutes, think about Syrians who were denied online payments for more than 3 [sic] years'.[27] This shows that non-state actors have also been targeted and are now targets in political cyber offensive operations. By targeting non-state actors, states are hoping to spread a very clear political message. However, in terms of the level of violence as defined by Khan, this author would argue that targeting non-state actors' website is less violent than targeting state actors. This is because of the fact that targeting a government website sends a stronger political message due to the fact that the website belongs to the government.

There is further evidence to suggest that states have used offensive cyber operations that have targeted how non-state actors' work. It can be seen that GCHQ has employed this technique against hacktivist groups. It appears that GCHQ targeted Anonymous as part of a cyber offensive operation that formed part of another operation termed Operation WEALTH which took place in the summer of 2011. It appears that the aim was to support law enforcement which is intelligence gathering, to disrupt Anonymous' communication which was in a DDoS attack which they termed operation ROLLING THUNDER, and it appears the operation was also aimed at trying to stop people supporting Anonymous.[28] Although it provides very little

[27] Syrian Electronic Army, @Official_SEA16, 'Twitter Feed', https://twitter.com/Official_SEA16/media, published 01.02.2014.
[28] Edward Snowden Document, GCHQ, 'Hacktivism: Online Covert Action', NBC News edited slide, ca. 2012, p. 14, Snowden Surveillance Archive.

information about the operation, it appears that ROLLING THUNDER was effective as the document provides a print screen of *Twitter* comments towards Anonymous that were hostile.[29] The document further states that the particular channel that was targeted by GCHQ had lost eighty per cent of its members by the end of the operation.[30] What this clearly shows is that GCHQ is targeting how non-state actors operate and that this is a way in which cyber offensive operations are taking place.

Publication Operations

A further type of operation that has taken place that is political is termed publication operations. This is again linked closely to a propaganda operation but falls into a category that is higher, in terms of violence, than propaganda. This is because, in a propaganda campaign, a state will simply spread messages, whereas, publication operations will often be higher due to how it is conducted and will often be linked to an ongoing situation.

An example of where this operation has been used against a state official will be discussed below. The purpose of this type of operation is to use cyber offensive operations to gather and then spread information that is highly damaging to a government. The information is gathered through accessing a system. The main use of this operation is that a government publishes information that is either damaging to a particular government or a government spreads a threat online claiming that if a particular action is not taken then the state will take action themselves. The purpose is to create political embarrassment or to force a government to change a policy. Although it includes the use of hacking, the purpose of the hacking is to gather information to allow it to be published. It may be that the information that a government releases is either out of date or is information that has very little intelligence value. This type of operation is likely to be infrequent in nature. This is because, once a government exposes the leaked information in the other country, the target country will look into the system that was affected. However, this is clearly a way in which states can use their cyber powers for an offensive operation.

It is not just states that have been targeted using publication operations as part of a political cyber offensive operation, but non-state actors have also been targeted in the same way. It is clear that there have been alleged cases of states placing

[29] Ibid., p. 14.
[30] Ibid., p. 15.

information in the public domain that had an effect on a company. This can be seen in the operation against *Sony Pictures Entertainment* in 2014-15. In this operation, it has been argued, around a terabyte of data had been taken from *Sony Pictures Entertainment*.[31] It was alleged that Sony was targeted by North Korea because of a film that they were making called 'The Interview' and in this film the main characters attempt to assassinate the North Korean leader Kim Jong-un. The actual aim of this attack will be covered later, but as a by-product of the operation, internal information about Sony was leaked and some of this information was problematic and could have affected relationships between film stars and business executives. For example, it was reported that a film producer told the co-chairperson of Sony that the famous actor Angela Jolie was 'out of her mind' because she had wanted to edit the script for the film Cleopatra.[32] The executive also asked for someone to 'Kill me please. [sic] Immediately' because Jolie wanted to change the director of 'Cleopatra'.[33] In addition, five films were also published online due to this operation.[34]

There are indications that this type of operation has also been contemplated for use against terrorist groups. One of the documents that was leaked by Snowden has argued that the NSA began to develop an operation that would target terrorist organisations by spreading information that had been collected about terrorist recruiters. This would lead people to question the terrorist recruiters' authority. It was argued that showing this information 'would call into question a radicalizer's devotion to the jihadist cause, leading to the degradation or loss of authority'.[35] The kind of information that they had completed publishing was the pornographic habits of recruiters, how these recruiters were using donations to fund their own lifestyle rather than the cause, the charges recruiters were demanding to speak at events, and when their language on a particular jihadist issue was not in keeping with the jihadist

[31] Sharp, 'Theorizing Cyber Coercion', 912
[32] Wikileaks document, 'Sony Emails', Email sent by Scott Rubin and Amy Pascal, 13.07.2014, https://wikileaks.org/sony/emails/emailid/32089, last accessed on 18.04.2016.
[33] Wikileaks document, 'Sony Emails', Email sent form Scott Rubin to Amy Pascal, 04.06.2014, https://wikileaks.org/sony/emails/emailid/50716, last accessed on 18.04.2016. C.F. This was not the only damaging information that was leaked. For more examples, see Sharp, 'Theorizing cyber coercion', 916.
[34] Andrew Griffin, 'Sony Pictures hack: Top films including Annie and Fury leaked, as Sony probes North Korea link', *The Independent*, first published on 01.12.2014, http://www.independent.co.uk/life-style/gadgets-and-tech/news/sony-pictures-hack-top-films-including-annie-and-fury-are-leaked-as-sony-probes-north-korea-link-9895443.html, last accessed on 02.12.2014.
[35] Edward Snowden Document, NSA, 'Memo: Islamic Radicalization', 03.10.2013, Snowden Surveillance Archive.

cause.[36] The NSA identified six different recruiters to target in this publication operation.[37] It is unclear whether this operation was actually used, or, if it was, how effective it has been. However, this document clearly shows that states can use this system to target terrorist organisations as well.

Target and Retaliation

A further type of cyber offensive operation that has a political objective is target and retaliation. This is because, in this type of operation, the main reason for conducting the operation is that a state will deliberately target an organisation or company to spread a political message, and that the operation is conducted in such a way that it is clear, though not provable, who conducted it. In this way, what the operation does is almost secondary to the fact that the operation is clearly visible. The aim is to conduct an operation in such a way that the general public suspect strongly that a particular state was involved in an attack but that they cannot prove it in concrete terms.

The operation targeting *Sony* is a prime example of this type of operation. In addition to the leaking of information, *Sony's* computer systems were targeted with a tool that wiped their systems and rendered them inoperable for six weeks.[38] It is also equally likely that this attack had another motivation. It could also be argued that in this operation, because it came at a time in which there was heightened tension between the US and North Korea, the aim was also to attack America but only in such a way that it would be indirectly attacking America. This is where the target of the operation would be important. Because the film industry, it could be argued, was and is such an important aspect of America life, by targeting this industry North Korea was able to affect the US state. This argument was supported by Admiral Rogers (Director of the NSA and Commander of US Cyber Command). Rogers states that in relation to the operation against *Sony*, it 'represents an attack against the very values of our nation, freedom of expression, you know, freedom of the media, freedom of the press'.[39] By targeting a non-state actor, there is a question about whether a state could,

[36] Ibid.
[37] Ibid.
[38] Christopher Joye, 'Australia launches cyber-weapons in global counter-terrorist operations', *The Australian Financial Review*, first published on 27.01.2015, http://www.afr.com/p/technology/australia_launches_cyber_weapons_hR1B30qv3c6bYKJvquVzo, last accessed on 27.01.2015
[39] Aspen Security Forum, 'Beyond The Build: Leveraging The Cyber Mission Force Aspen', David Sanger *The New York Times* and Michael Rogers, Director National Security Agency, Commander, U.S. Cyber Command July 23, 2015 Transcript p. 35.

or should respond to this in the same manner as if a state was targeted directly. This is because, as they were not targeting a business that was seen as vitally important to the national security of the US, they would be less likely to respond militarily. In addition to this, the target of Sony being so public, it could be argued that a further aim would be that they could create a fear of a country by targeting something that is so public. In this case, the aim would be to demonstrate what a state can destroy within an organisation and that they can do even more damage. In this way, the aim is to threaten a state but just do so indirectly.

Another example of this type of activity that have been linked to a state but has targeted a non-state actor was the targeting of Las Vegas Sands Corp Casino in America. This was conducted by the Iranians and it can be seen to have a political message. It has been argued that the reason that this company was attacked was because the Chairman of this company was Sheldon Adelson who was a supporter of Israel and had spoken critically about Iran.[40] This meant that the aim of the target was not so much to cause a financial issue, although as will be covered in the next chapter, it did, but the main aim appears to have been to target those who have spoken out against Iran. In this way, it shows that states can and are targeting companies whose leaders are against what they stand for. This means that the target of the attack is very important. It is not the only time in which it has been argued that Iran has targeted businesses to spread a political message.

In 2012, Iran launched a number of DDoS operations against American banks.[41] It has been argued that the reason for such operations was due to the fact that the US had been involved in economic sanctions against Iran.[42] In this way, the reason for targeting banks is clear. It sends a message that, if America affect the Iranian economy Iran can affect Americas. Although the actual economic effect that was caused in this case was minimal, if any at all, as will be discussed later, the idea

[40] Tony Capaccio, David Lerman, and Chris Strohm, 'Iran Behind Cyber-Attack on Adelson's Sands Corp. , Clapper Says', *Bloomberg*, first published on 26.02.2015, http://www.bloomberg.com/news/articles/2015-02-26/iran-behind-cyber-attack-on-adelson-s-sands-corp-clapper-says, last accessed on 27.02.2015.
[41] Edward Snowden Document, NSA, 'Memo: Iran- Current Topics, Interaction with GCHQ', from NSA S2E4 Iran Division Chief to S2E Foreign Partner Strategist, dated 12.04.2013, paragraph one, Snowden Surveillance Archive.
[42] Ellen Nakashima, 'Iran blamed for cyberattacks on U.S. banks and companies', *The Washington Post* first published on 21.09.2012, http://www.washingtonpost.com/world/national-security/iran-blamed-for-cyberattacks/2012/09/21/afbe2be4-0412-11e2-9b24-ff730c7f6312_story.html, last accessed on 16.02.2015.

of targeting the American banks could be argued was aimed at sending a clear political message.

Furthermore, it has been argued that Iran has targeted oil companies in states that have been supporting oil sanctions against Iran.[43] This then shows that an attempt was made to try and force a state to change its policy towards Iran by not targeting another state directly but by targeting a business. In one such case, Iran was believed to have attacked the oil industry by launching a virus that wiped the systems of an oil company and caused the system to be offline for around two weeks. As this company was part of a country that took part, along with other Middle Eastern countries, in the sanctions against Iran.[44] It could be argued that this clearly shows that the target of the attacks was chosen to send a political message as part of the sanctions were to stop the buying of Iranian oil. This means that the attack was a cyber offensive operation that was designed to send a political message because of what they targeted, and it was also retaliation. This shows how states were and can target businesses in a cyber offensive operation.

Resentment Campaign and Misinformation Campaign

A further way in which political cyber offensive operations can be conducted is through the spreading of resentment and misinformation. A resentment campaign aims to cause a group inside a country to believe that a government is not working for them, therefore causing this group to question that government. A resentment campaign is not likely to be used to create resentment in the sense that an operation is unlikely to be able to make people who absolutely support a government suddenly change to hating a government. The purpose of a resentment campaign is to amplify the feelings of those who are already disaffected with a government or are beginning to question a government.

There are several ways that these types of operations can and have taken place. There have also been cases where groups have allegedly looked to fake high profile news stories that, it could be argued, could be used to try and destabilise countries. It can be seen that this operation has taken place. This can be seen in the fact that it was reported that a campaign was conducted by a group with links to the Russian government. This group spread a story that a chemical plant had exploded

[43] Ibid.
[44] Rid, *Cyber War Will Not Take Place*, p. 55f.

and more importantly, that it aimed to persuade people which police officers in Atlanta had killed an unarmed black woman. This appears to try and focus on and add to the domestic issues that the US was facing at the time after the shooting of an unarmed black teenager in Ferguson, Missouri in 2014.[45] The same group were also allegedly used to spread a story about a leak at a chemical plant and that Ebola was spreading throughout the US.[46] However, the chemical plant seems to have been an operation that was easy to counter. The most damaging one of these stories appears to be the story of the killing of the unarmed black woman. If this was conducted by Russia, it could be argued that this could be a cyber offensive operation and that it is political because it was aimed to spread resentment. Even if this was not, conducted by Russia, it does show a way in which cyber offensive operations could be used to try and destabilise a country, as an organisation is looking to create resentment and discord within a population and it is possible that this could cause political instability within a country.

Furthermore, it is clear that GCHQ has developed a number of tools that could be used to help spread resentment. There have been several tools that were developed by GCHQ called CLEANSWEEP. The purpose of this tool was to allow GCHQ to change the outcome of online polls.[47] Although this may seem like a tool that would have very little actual benefit, if GCHQ could change the outcome of an opinion poll that was used to conduct of survey of a policy that the British government disagreed with they could then 'show' that a political party in a country went against the wishes of the people that could be used to spread discontent within a population. Another tool was called BADGER. This has the ability to send out mass messages using emails.[48] It could be used for cyber intelligence purposes if it were infected with a virus that contained malware designed to gather intelligence. But it also has the ability to be used for a political campaign. This is because if the message was tailored in a certain way it could create resentment towards a particular government or person. A government could use it to send out hostile messages towards another state. There is

[45] Adrian Chen, 'The Agency From a nondescript office building in St. Petersburg, Russia, an army of well-paid "trolls" has tried to wreak havoc all around the Internet — and in real-life American communities.' *The New York Times Magazine*, first published on 02.06.2015, http://www.nytimes.com/2015/06/07/magazine/the-agency.html?smid=nytcore-ipad-share&smprod=nytcore-ipad&_r=0, last accessed on 03.06.2015.
[46] Ibid.
[47] Edward Snowden Document, GCHQ, 'JTRIG Tools and Techniques', 05.07.2012, p. 5, Snowden Surveillance Archive.
[48] Ibid., p. 5.

also a tool termed CONCRETE DONKEY, which can 'scatter an audio message to a large number telephones or repeatedly bomb a target number with the same message'.[49] Although targeting a phone does not seem to be cyber activity, it must be noted that because of the increase in smartphone usage it could be, if conducted in the right way, a type of cyber offensive operation. This is, again, because it is a way to spread resentment. PITBULL, although it was under development, had the ability to send a tailored message to those who are using Instant Messaging Services.[50] This means that if the operation was conducted in a way that it sent out a message about a protest, or an activity of a state directed towards a particular group, it could then help to further destabilise a government. What this clearly shows is that GCHQ have developed tools that allows them to foster resentment.

A further political use of cyber offensive operations is through the spreading of misinformation. This type of operation is different from the publication type of operation because the objective here is to cause problems for someone who is linked to the heads of state or has power but is not actually the head of state. The objective here is to cause those who are in power to question the loyalty of a particular person. This can have a number of objectives. It can cause there to be questions about a particular organisation of state control like a ministry. It would do this by spreading information that a person or people were disloyal to a government. If directed at an authoritarian country, it could cause a person to be executed. It is clear that GCHQ have developed the tools to conduct this type of operation. SCRAPHEAP CHALLENGE has the ability, as GCHQ stated, to 'perfect spoofing of email from targets using a Blackberry'.[51] If this were used in a certain way, GCHQ would have the ability to make it appear that a person sent an email to someone. Along with this, as was mentioned above, GCHQ had the tool termed CLEAN SWEEP, which had the ability to post information on someone's Facebook page.[52] This type of tool would allow an intelligence organisation to plant information that suggests that a person or a group of people are disloyal to the controlling party by planting information which shows they were doing things that were not in support of a party. A further tool that GCHQ developed had the ability to encrypt files so people could not access them. If

[49] Ibid., p. 5.
[50] Ibid., p. 5.
[51] Ibid., p. 6.
[52] Ibid., p. 5.

this was used in a campaign which looked to show someone might have been disloyal it could provide 'evidence' that this person was looking to hide information. There have been cases where it is clear that GCHQ appear to have actually conducted this type of campaign. Much as was the case with the military deception, many different forms of activities beyond cyber offensive operations could be used to spread the evidence that someone is disloyal to make it more effective. It is not clear if any of these operations have actually taken place, as the tools have been described as either 'ready to fire' or 'near ready'.

There is no reason to believe that the forms of operation that were mentioned above could not be used against terrorist organisations. They could be used to target them by spreading resentment designed to convince the organisation that a person working for them is about to defect, working for an enemy intelligence organisation, or is working for a rival terrorist organisation. This is much the same operation as was discussed about the spreading of actual information about terrorist recruiters, however the aims here are to spread information that would be untrue. Although this author cannot find any evidence that this type of operation has actually taken place, it is clearly a way in which a state could look to conduct a cyber offensive operation against terrorist organisations.

Voting Systems

The final form of political cyber offensive operation is achieved by targeting the voting systems of a particular country. Although there has been no actual evidence of this form of operation taking place in which votes were actually changed, there is a chance that political cyber offensive operations could be used to change voter tallies in an election.

There is evidence that the Russians conducted operations in which they targeted voter information. It has been argued by Sam Liles (Acting Director from the Office Of Intelligence and Analysis Cyber Division, Department Of Homeland Security), that at no point were votes changed.[53] Although it has been argued that influencing voters by conducting offensive operations would be very difficult, and in some places impossible, there is still a risk that at some point in the future, a cyber

[53] Sam Liles, Acting Director, Office Of Intelligence And Analysis Cyber Division Department Of Homeland Security, Senate Select Committee on Intelligence 'Hearing On Russian Interference In 2016 Election, Panel 1', *Political Transcript Wire*, 21 June 2017.

offensive operation may be able to do this. This has been one of the reasons that some countries have in recent elections removed online voting. It was argued that in a situation where there is no paper voting system or the voting machines run outdated software, it may be possible to change votes in an election.[54]

In addition, it was noted that changing votes would not be impossible, it is that it would become visible.[55] However, even if such operations were actually detected there may be another reason to conduct such operations. For example, if a state aimed at trying to convince others that a fraud was taking place in the election, or that a system of government was not effective then changing votes with the understanding that this will become known could have, it is possible, a highly damaging effect. In this case the operation would not be aimed at winning the election, but aimed at showing the election was a fraud. It was argued by Senator Rubio that these types of operations would have damaging results.[56] From this it could be that by simply affecting the systems, a political objective may be achieved. Further, by accessing voter information, other forms of political operations can take place. It is possible that voters could be denied the right to vote because they have been removed from the electoral register or their address has been changed. This then could change the outcome of an election. In this way, political cyber offensive operations could be conducted in such a way that votes of an election were either changed or were affected in some other way.

Complete Operations

There have been a number of political cyber offensive operations that have taken place that can be seen to have used several of the techniques that have been looked at in this chapter. This allows for an assessment to be made on the operations as a whole. There was Russian interference in the US presidential elections in 2016 and Russian interference in other European elections, most notably the French election in 2017. In terms of Russian interference in the US election, all the information is still not known. At the time of writing this thesis, the Senate Select Committee of

[54] James Scott and Drew Spaniel, 'Hacking Elections is Easy! Part 1: Tactics, Techniques, and Procedures', *Institute for Critical Infrastructure*, September 2016.
[55] Sam Liles, Acting Director, Office Of Intelligence And Analysis Cyber Division Department Of Homeland Security, Senate Select Committee on Intelligence 'Hearing On Russian Interference In 2016 Election, Panel 1', *Political Transcript Wire*, 21 June 2017.
[56] Senator Mark Rubio Senate Select Committee On Intelligence 'Hearing On Russian Interference In 2016 Election, Panel 1' *Political Transcript Wire*, 21 June 2017.

Intelligence investigation was still ongoing. Further, there have not been any publications from the House Permanent Select Committee on Intelligence as their work is also still ongoing. Finally, there was, and at the time of writing this, a still ongoing investigation by the Special Prosecutor Robert Mueller (former director of the Federal Bureau of Investigation) who is tasked with investigating whether there were any connections between President Donald Trump's campaign team during the election and Russian interference. As these investigations do have the ability to see and hear classified information, it is possible that new evidence will come to light when these all produce their reports. However, from the various hearings of both intelligence committees there is enough evidence to understand Russian interference in the US elections. This is helped because the CIA, the FBI, and the NSA produced an unclassified assessment of Russian involvement in the US elections. Although this is a lot shorter than the classified version, there are still many details contained within this document to provide the evidence that is needed to understand Russia's use of cyber offensive operations for a political campaign.

It appears that the cyber offensive operation formed part of a larger campaign that also included non-cyber activities (this is covered in chapter five). However, the cyber offensive operations have a number of different elements to them. It included propaganda as part of the campaign. These propaganda campaigns featured, for example, the allegation that Presidential nominee Clinton was unwell and would be unfit to take office. Further, there is clear evidence that Russia used paid trolls to spread propaganda about Clinton. The Russians have developed an organisation called the Internet Research Agency that, it was argued, had ties to Russian intelligence. This organisation housed paid professional trolls who would spread stories. At the same time as degrading Hillary Clinton, it has been claimed that these trolls also spread pro-Donald Trump messages.[57] In addition to paid human trolls, they also used *Twitter* bots to further conduct their social media propaganda campaign.[58] Finally, these paid trolls were also used in conjunction with other propaganda efforts. They would be used to amplify and spread information and stories that would fit in with degrading Clinton and supporting Trump.

[57] Office of the Director of National Intelligence, 'Intelligence Community Assessment Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution', 6 January 2017, p. 6.
[58] Senator Mark Warner, Senate Select Committee On Intelligence 'Hearing On Russian Intervention In European Elections', *Political Transcript Wire*; 28 June 2017.

Another way in which this campaign was launched was through groups that may or may not have been Russian intelligence to access the systems of the Democratic National Convention (DNC) and the Democratic Congressional Campaign Committee. The Russian government gained access to the DNC from around July 2015 but this access was only discovered in June 2016. Three US intelligence agencies stated that one of the Russian organisations that was discovered in the DNC network was the General Staff Main Intelligence Directorate (GRU) (the intelligence community have not stated which other Russian organisation was inside the DNC network at the same time as the GRU). When the Russians had gained access to the system they began to extract a large amount of information including private emails from Clinton and her campaign manager John Podesta. These were given to various websites including *Wikileaks* and DCLeaks.com. DCLeaks.com is a website that publishes leaked information about the US government. There is no evidence that the Russians had tried to change any of the information that was leaked.[59] It appears that the Russians gave this information to the sites because they had some level of standing and it would mean that Russia could maintain some level of deniability about being involved in the operations. In these ways, it is clear that part of the cyber offensive operation conducted by Russia included leaking of damaging information.

The final way that it appears this operation was conducted, or at least one the ways that the Russians had tried to conduct the operation, was through targeting state and local election boards and voting systems.[60] There is no evidence that any votes were changed, which was one of the key features of both the House Permanent Select Committee on Intelligence and the Senate Select Committee of Intelligence investigations. This is partly because it has been stated that it would have become clear that this had happened. It is not clear whether Russia had actually considered changing votes but could not do so, or whether they had no intention of having this as part of their broader campaign. However, at least nineteen states election boards were targeted. It has been argued that there are many reasons why Russia may have

[59] FBI Director Jim Comey, (Appears to be mislabelled in their transcript) Senate Select Committee On Intelligence 'Hearing On Russian Intelligence Activities', 10.01.2017, *Political Transcript Wire,* 11.01.2017.
[60] Office of the Director of National Intelligence, 'Intelligence Community Assessment Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution' 6 01.2017, p. 6.

targeted these systems other than to change votes. One of the reasons may have been to help them to create a phishing scam where they would need other information, or using the data to send out targeted messages as part of their operation to interfere in the US election.[61] From this, the campaign to discredit Hillary Clinton in the eyes of the US electorate could have been more targeted and achieved better results.

It has been argued by the joint intelligence assessment that the Russian political cyber offensive operation had three main goals. They wanted 'to undermine public faith in the US democratic process', they wanted to 'denigrate Secretary Clinton, and harm her electability and potential presidency' and they developed a strong preference for Donald Trump, which would indicate that they wanted him to win.[62] However, this author disagrees with some of the conclusions of the US intelligence agencies about the aims of the Russian cyber offensive operation and the fact that Russia had achieved these aims.

On the objective of undermining the democratic process this author agrees with their assessment. It could be argued that Russia has been very successful in its operation. This is due to the fact that these activities are still being investigated and the political fallout is still being felt that this has helped to undermine the US democratic process. In addition, there were a number of stories placed about the idea that if President Donald Trump was not elected president it was caused by the fact that the election was rigged. This is also supported by the fact that now it is possible that whenever an election result does not turn out the way that it is hoped people now have the ability to claim that the election was affected by an outside power.

Further, by the fact that in Europe a number of democratic elections have or are taking place, if Russia was shown to have had some effect on these elections it helps to undermine not only the US democratic process but also the democratic processes throughout the West. Labour MP Ben Bradshaw (Exeter) stated that 'We have not even begun to wake up to Russia's cyber-warfare. Its interference in the American presidential elections is now proven. It probably interfered in our own referendum' although he argued that 'we do not have the evidence for that yet, but it

[61] Bill Priestap, Assistant Director, FBI Counterintelligence Division, Senate Select Committee On Intelligence 'Hearing on Russian Interference in 2016 Election, Panel 1' 21.06.2017 *Political Transcript Wire*; 21 June 2017.
[62] Office of the Director of National Intelligence, 'Intelligence Community Assessment Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution' 6.01.2017, p. ii.

is highly probable'.[63] Overall, then it is clear that Russia succeeded in undermining democracy.

However, the conclusion that the Russian operation was designed to directly get President Donald Trump elected is much harder to prove. The joint intelligence assessment states that 'Putin and the Russian Government aspired to help President-elect Trump's election chances when possible by discrediting Secretary Clinton and publicly contrasting her unfavourably to him'.[64] Although this was the judgment of all three agencies, and one they all agreed, the CIA and FBI have high confidence in this judgment; NSA had moderate confidence.[65] It is clear that the Russians disliked Hillary Clinton. It has been argued that this was caused when Russian President Vladimir Putin publicly blamed Clinton 'for inciting mass protests against his regime in late 2011 and early 2012, and because he holds a grudge for comments he almost certainly saw as disparaging him'.[66] However, this is a little different from actually wanting Donald Trump to win the election. It is this author's opinion that overall, based on the evidence that is available, Russia did not actually care if Donald Trump won the election. Instead their main aim was to avoid Hillary Clinton being elected and for her reputation to be damaged. The best way that a political operation could target a candidate they did not like would be through providing the opposition some help. Even if there were some level of coordination between Donald Trump's campaign and Russia, this does not prove that Russia wanted Trump to win the election. At the point of writing the only member of Trump's campaign team to be shown to have had contact with Russia was Donald Trump Jr.[67] This contact it has been alleged was so that Russia could give information to Trump's campaign that was damaging to Hillary Clinton. Even this would show that Russia wanted to undermine Hillary Clinton. It also shows that Donald Trump's campaign was willing to accept help.

---

[63] Ben Bradshaw, 'Aleppo/Syria: International Action 13 December 2016 Volume 618' *Emergency debate (Standing Order No. 24),* https://hansard.parliament.uk/Commons/2016-12-13/debates/16121344000001/AleppoSyriaInternationalAction#contribution-935FBA3F-3657-4CAE-9743-5A488A0204FE, paragraph 652-654.

[64] Office of the Director of National Intelligence ,'Intelligence Community Assessment Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution', 06.01.2017, p. ii.

[65] Ibid., p. ii.

[66] Ibid., p. ii.

[67] David Smith, Ben Jacobs, Jon Swaine, Shaun Walker, 'Trump Jr was told of Russian efforts to help campaign – report', *The Guardian*, first published on 11.07.2017, https://www.theguardian.com/us-news/2017/jul/10/donald-trump-jr-russia-meeting-clinton-statements, last accessed on 11.07.2017.

Even if Russia had wanted and actively approached the operation with the aim of getting Donald Trump elected, it is still unclear whether they succeeded. It is possible that other factors around the presidential race allowed Donald Trump to be elected. Firstly, it is possible that due to the fact that both candidates were unpopular people did not vote as usual. Secondly, the FBI reopened an investigation into Hillary Clinton's use of a private server for her government emails. The final factor that may have affected the outcome of the results of the US election is the electoral process that the US uses. This is because in the US, the presidential candidate must win in terms of number of votes of the electors from the state rather than the number of people that voted for them nationwide. The electors are governed by how many members each state, including the District of Colombia has in Congress. This meant that although Hillary Clinton had the most votes nationwide, she did not win due to the electoral system in the US. All of these issues, it could be argued, had a much bigger impact on the election than Russian involvement.

Further, Donald Trump was unpopular throughout the world. One of the motivations for this operation was to undermine both western and American democracy. From this, it could be argued, what better way to show the flaws of democracy than showing the world candidate Donald Trump. This is supported by one of the hearings into Russian interference. Senator Cotton asked the former Director of National intelligence (James Clapper) 'Did he [Putin] or the intelligence services ever believe that Donald Trump was a likely winner?'[68] Clapper responded with 'Initially, no. They thought he [President Trump] was a fringe candidate and didn't think that at all'.[69] This would then mean that the Russians were much more concerned with weakening democracy than actually helping Trump. In these ways, the author would argue, that the motive was not to help candidate Donald Trump but was merely to weaken Hillary Clinton.

Other Elections

In addition to Russian involvement in the US elections, it is clear that they have been involved in other elections especially in Europe. Russia appears to have conducted similar operations against other elections, including the French presidential election of

[68] Senator Tom Cotton, Senate Select Committee On Intelligence 'Hearing On Russian Intelligence Activities' 10.01.2017, *Political Transcript Wire*, 11.01.2017.
[69] James Clapper, Director Of National Intelligence, Senate Select Committee On Intelligence 'Hearing On Russian Intelligence Activities' 10.01.2017, *Political Transcript Wire*, 11.01.2017.

2017. This includes the fact that they stole information about the then candidate Emmanuel Macron and released it, much the same way as they did against Hillary Clinton.[70] They also spread fake news stories about Macron. Further, they supported Macron's opponent, Marie Le Pen, by providing support and financial assistance. It has not just been the French elections where it has been alleged that Russia has become involved. It was argued that Russia has tried to influence 'the Montenegrin [and] Dutch,' elections. [71] Further, it is also possible that the Russians are planning to become involved in the German elections of 2017, as it was noted that the German parliament suffered a major cyber incident in which emails were stolen and it is expected that around the time of the German election, these will be leaked by the Russians. [72]

Examining what could be argued to be a complete political cyber offensive operation is important because it shows that these operations are not isolated and can be conducted in many ways. In the example of the elections that were examined above, Russia has used publication operations, disinformation and voter system operations. In these ways, political cyber offensive operations are clearly taking place.

Comparison

It can clearly be seen that a direct connection exists between traditional covert action and cyber offensive operations that are aimed at conducting political activities. Firstly, both types of activities have in the past targeted both states and non-state actors. In this way, the choice of target does not distinguish one type of activity from the other.

A further comparison can be drawn in the fact that both covert action and cyber offensive operations have used a multitude of different ways to target an adversary. In traditional covert action, states have recruited agents of influence or they have tried to affect the political outcomes of elections. It can be seen that some of the cyber offensive operations that have taken place are the same as those that have

[70] Wikileaks document, 'Macron Campaign Emails', https://wikileaks.org/macron-emails/.
[71] Nicholas Burns, Professor, Practice Of Diplomacy And International Relations, Harvard Kennedy School Of Government, Senate Select Committee on Intelligence 'Open Hearing: Russian Intervention in European Elections', 28.06.2017, *Political Transcript Wire*, 28.06.2017.
[72] Senator Mark Warner, Senate Select Committee on Intelligence 'Open Hearing: Russian Intervention in European Elections' 28.06.2017, *Political Transcript Wire*, 28.06.2017.

taken place in the past. For example, publications operations were shown to have been used before and the use of them as a tool for cyber offensive operations clearly demonstrates the comparison between the two types of activities. The resentment campaigns can be seen to have, at the very least, been envisaged to be used against the Soviet Union. The use of political activities to affect elections can also be seen to have taken place in the past. Even though there has at this point been no evidence of voting systems being affected to change the outcome of an election, this does not mean that it will not happen. In these ways, it is clear that cyber offensive operations and covert action, in terms of some of the types of activities can be seen, to follow the same pattern.

In cyber offensive operations they have attempted to use 'new' types of activities to attempt to send political messages. However, overall, the difference the 'new' aspect of cyber offensive operations is how they target another state rather than the activity being in any way new. This argument is also supported by the fact that there are some types of political activities that if a state wished to conduct against an adversary they would have to use traditional covert action such as an agent of influence. This then adds additional evidence that the 'new' versions of cyber offensive operations are only new in how they target another adversary rather than the actions themselves being particularly new. All of these activities have been designed to affect the power and policies of another country.[73] In these ways, a direct connection between cyber offensive operations and covert action exists when the actions are political.

Conclusion

This chapter has clearly demonstrated that there is a clear connection between covert action and cyber offensive operations that are political in nature. This argument was clearly demonstrated by the fact that firstly some cyber offensive operations that have taken place that are political can be seen to have taken place in the past. This argument was highlighted by examining past covert action campaigns that can be seen and were aimed at affecting a state or non-state actor politically. Further, highlighting the number of ways that states have used covert action in the past to target others

[73] Rositzke, *The CIA's Secret Operations*, p. 185.

politically shows that the actions are not new, it is just the method or the delivery system for the operations that are new.

This chapter has argued that states have conducted political cyber offensive operations that include defacement; where a state defaces a website, stopping websites from working; states stop websites from functioning to create a political message, retaliation operations; where a operation is conducted it such a way that it is clear which state has do the operation to send a political message, a publication operation; where a state will publish damaging political information, and finally, resentment campaigns; where a state aims at creating or heightening tensions within a chosen state or terrorist organisation. It has also argued that it is possible that political cyber offensive operations could be conducted in such a way that they affect voting systems. Finally, this chapter has looked at a complete political cyber offensive operation that contained multiple political cyber offensive components. In these ways, this chapter has demonstrated four of the six overarching ways that states can use cyber offensive operations to target both state and non-state actors.

CHAPTER FOUR

Covert Action and Cyber Offensive Operations: A Comparison between Economic and Paramilitary Operations

This chapter will address the two final forms of covert action and cyber offensive operations that states can use against other states as well as non-state actors. The two forms of operations that will be looked at are economic operations and paramilitary operations. This chapter will argue that it can clearly be seen that there is a direct connection between cyber offensive operation and covert action in terms of economic operations and paramilitary operations.

Further, this chapter will clearly demonstrate that cyber offensive operations can be used to conduct economic operations. It will argue that there are six overarching ways in which economic cyber offensive operations can take place: stopping banking websites, targeting personal accounts, targeting business accounts, effects of cyber operations, cyber heist and, finally, spreading information. The final area of cyber offensive powers that will be looked at is what could be termed high-end operations. This is where cyber offensive operations are used for the most violent form. The main way that these operations are conducted is focused on stopping something from working. However, they could also be conducted in other ways. The purpose in these forms of operations have a number of objectives which rangers from individual operations, where you disturb a single person, stopping services from working, the use of cyber offensive operations to conduct assassination and, finally, targeting of critical national infrastructure. What links them together is that they are the most violent forms of operations and where, it could be argued, that states come closest to committing an act of war.

Within this area of operation, there has been a tendency to focus on worst-case scenario ideas. This is because there is much speculation about this type of operation and this can lead to misreporting of events. This is because it is under this heading where the targeting of critical national infrastructure would take place. There have been reports about cyber being used to cause a Cyber Armageddon and a Cyber Pearl Harbor. The idea of Cyber Pearl Harbor is that a cyber offensive operation could be

launched out of the blue that would have such destructive effects that it could disrupt people's way of life by destroying power stations or even kill them.[1] Yet, although these operations are those that have the ability to disrupt power stations, there are other forms as well. In these ways, this chapter will demonstrate that economic and high-end operations are two ways in which cyber offensive operations can be conducted against other states as well as non-state actors.

The final part of this chapter will clearly show that when these economic operations and the use of high-end operations are compared to economic operations and paramilitary operations in the past, it clearly demonstrates the direct connection between covert action and cyber offensive operations in these types of activities.

Traditional Covert Action: Economic Activities

Economic operations aim to undermine a country's economic power. These actions are very much interlinked with political covert action because by undermining a state's economic power, a state could cause the domestic population to question the effectiveness of the power that is in control of their country. Although this author has not come across any examples of economic activity being used against terrorist organisations, there is no reason to believe that they cannot be used.

The use of economic operations can also take place by considering ways in which they could undermine economic conditions in a target country. This was a particularly important area of study that the British paid a lot of attention to during the early part of the Cold War. In the meeting of the Committee of Communism Overseas, there were various studies in which the British looked into how operations could be conducted to affect the economies of various countries under the influence of the Soviet Union, most notably the Czechoslovakian economy. They also looked at what could be done in other parts of the Soviet bloc. The operations that were discussed were to increase unrest in the labour force, either by increasing the tensions that were felt towards communism, or even playing into national hostilities that countries felt toward each other. This included adding to friction between Polish and

[1] James J. Wirtz, 'The Cyber Pearl Harbor', *Intelligence and National Security*, 32:6, (2017), 758-767 758, C.F. This author does not believe in Cyber Pearl Harbor but summaries effectively. See also, Leon Panetta, Former United States of America Secretary of Defence, quoted from Alex Spillius, 'US at risk of 'cyber-Pearl Harbor', Leon Panetta warns' *The Telegraph*, first published 12.10.2012, http://www.telegraph.co.uk/news/worldnews/northamerica/usa/9604794/US-at-risk-of-cyber-Pearl-Harbor-Leon-Panetta-warns.html, last accessed on 04.02.2015.

Czech countries.[2] They also looked at targeting the economies by denying equipment that would, if it were provided, help the economies.[3] However, there is no evidence yet to indicate that the plans were ever actually carried out. These plans seem to have been abandoned when it was noted that other parts of the Soviet Union could probably deal with these issues and that, even if the items were not exported to the west, they would be bought by other parts of the Soviet Union, thus not causing there to be much in terms of economic effect. Nevertheless, although they did not take place, it does clearly show ways in which economic operations could be conducted. This is because the plans were such that they were designed to affect the economies of this country and could have been used against other countries. This also shows another way in which covert economic action can take place where, instead of one country acting alone, they and persuade other countries to try and apply economic pressure. This is different from overt economic pressure as the aim is to make it appear that the other countries have conducted this on their own or even to make them not admit that they have done so.

States have, at times, looked at ways in which they could apply covert economic pressure to a country by using private companies. In a revised plan to target Guatemala in 1953-1954, the CIA used private companies to achieve this aim of undermining the economic stability of Guatemala. It was noted that they planned to use an 'already cleared group of top ranking American businessmen in New York city' to create shortages of imports and cut the level of exports that Guatemala were able to conduct.[4] This type of operation also seems to have been planned to take place in Chile when the CIA used American businesses with interests in this to apply economic pressure. It was noted that in the 1970s, US private investment amounted to around 1.1 billion dollars and this was after Chile had tried to diversify their debt.[5] What these operations do show is that states can use private companies to apply economic pressure to another country. In these types of covert action, the aim is to affect the economic conditions abroad in such a way that it is the domestic population

[2] TNA, CAB 134/3, 'Official Committee of Communism Overseas', The Vulnerability of Satellite economy to external and internal pressure report prepared by the Ministry of Defence, JIB and Foreign Office EID B.14/G.3, pp. 1-3.
[3] Ibid., pp. 1-3.
[4] Nick Cullather, *Secret History: The CIA's Classified Account of its operations in Guatemala*, Second Edition (Stanford: Stanford University Press, 2006), p. 41.
[5] Ibid., p. 33.

of the country that is being targeted.[6] In this way, it creates a great deal of unrest for the population, which in turn could either cause a change of government or force the target country to change a policy.

In these ways, states have used economic covert action operations to target other states in a number of ways. This includes denying equipment that would, if it were provided, help the economies of specific countries to grow. In addition, states have used private companies to further apply economic pressure on states.

Cyber Offensive Operations: Economic operations

Cyber offensive operations have been used to conduct economic operations. There are many ways in which they could be used in the future that can be seen to have a direct economic effect. Most of the instances of the actual use of economic cyber offensive operations that will be illustrated in this chapter have targeted non-state actors, though these have not usually been conducted against terrorist organisations. This author would argue that states will target non-state actors because it is possible that much economic harm can be achieved against another state through targeting non-state actors such as businesses. Further, by states using these operations to target businesses, it shows they have the ability to produce economic harm to a state but doing it in such a way that it is indirect. This presents a benefit to states in conducting these types of operations. This is because it becomes difficult for states to claim that they have been directly targeted by another state as they are not targeting state controlled assets. Some of the ways in which a state can conduct economic cyber offensive operations are very similar to that of criminal organisations. However, the reason for conducting the operations is what is different here. The operations are not conducted to produce individual profit and that is what makes it different from criminal operations, even if they were conducted by states, as was the case with the Ransomware virus WannaCry that has been linked to North Korea. [7]

There are many reasons to conduct a cyber offensive operation that produces economic harm. It has become increasingly clear that banks and other financial institutions have been targeted. In the US, more than a hundred financial institutions

[6] Lowenthal, *Intelligence*, Seventh Edition, p. 256.
[7] Gordon Corera, 'NHS cyber-attack was 'launched from North Korea'', *BBC News*, first published on 16.06.2017, http://www.bbc.co.uk/news/technology-40297493, last accessed on 16.06.2017.

based in Wall Street suffered some form of cyber related incident in 2015.[8] However, although most of these incidents are likely to have either been from criminal organisations, or if they were conducted by a state, would most likely have been related to the gathering of intelligence, it is possible that a state could seek to conduct an economic cyber offensive operation. Furthermore, there are many different ways in which this type of operations could and, in some cases appear, to have been conducted. Although, the operations that have been looked at have focused on how states could conduct economic operations against states, but indirectly, there are, however, some operations that if conducted by states could be used to target terrorist organisations as well.

Denial of service

A denial of service attack is, in this author's opinion, the lowest level of violence that an economic operation can take. It can be achieved through the use DoS or a DDoS as discussed in the previous chapter. Further, at this stage these types of operations have only reached the level of annoyance rather than actually producing much, if any, economic harm.

Yet, it has been suggested that these types of attack should actually be seen as more damaging.[9] These operations have the ability, in theory, to have some major consequence. The reason that at this point they are the lowest level of violence in terms of economic operations is because the examples of these types of operations have occurred over a short time frame and have not been sustained for long periods of time. This was noted by Rid, who examined one of the longest sustained DDoS attacks against banking systems against the Estonia bank Hanspank lasted for around ninety minutes one day and two hours the next day.[10] There are further examples of DDoS operations being used for economic operation. Between 2011 and 2013 a number of denial of service attacks were launched against a number of banks and financial institutions based in the US. The use of DDoS attacks that stopped the websites of more than forty-six different organisations, most of these against US

[8] Matthew Goldstein, 'Firms Wary of Breaches by Hackers, Not Terrorists', *The New York Times* first published on 04.02.2015, accessed via Nexis Business and News.
[9] Clarke and Knake *Cyber War*, pp. 14-16, C.F these authors rather than stating this imply it with their language of a change from annoyance.
[10] Rid, *Cyber War Will Not Take Place*, p. 6.

financial institutions.[11] The group behind these activities, which the US termed ITSec Team, was linked directly to the Iranian Republican Guard Corp. These attacks were launched against, *Bank of America*, *Capital One Bank*, *ING Bank NYSE*, and others. It was argued that these attacks were 'designed to undermine the business of these companies'.[12] These attacks meant that customers were unable to conduct online transfers. However, it must be noted that at this point in time, this type of operation is likely to have very little actual effects beyond being an annoyance. This is because a state is stopping a bank from conducting online transfers or stopping people from being able to access their online accounts. The only actual economic effects that this type of operation could have would be that if banks had important transfers that were needed then. This would mean that they could stop these from taking place. In addition, by targeting the *New York Stock Exchange*, an operation may achieve some economic harm by stopping investments from being made. However, these types of operations are difficult to sustain over a long period of time. This is because, once a bank knows that this type of operation is happening, they would then look to try and counter-act this. Even in the case of the ITSec Team, it was not over years that these operations were taking place but over a short time period. This would mean that the actual economic effect was likely to be minimal. Nevertheless, these operations do show ways in which states can target other states use economic cyber offensive operations. It could be argued that these types of activities, could almost be seen as a form of economic warning shot, in which they are designed to create an economic annoyance rather than anything else.

Denial of service attacks could also be conducted against businesses that are not banks or financial institutions. Again, the point would be to stop the business from being able to conduct online transfers. An example of this type of attack occurred when the Syrian Electronic Army launched a denial of service attack against *eBay* and *PayPal*.[13] The main reason for these attacks was discussed above, however, it is clear that these types of operations could, by targeting businesses, affect their economic stability if they are reliant on online transactions and it could, if conducted over a long

[11] United States District Court Southern District of New York, 'United States v. Ahmad Fathi, Hamid Firoozi, Amin Shokohi, Sadech Ahmadzadegan a/k/a "Nitr0jen26, Omid Ghaffarinia a/k/a "PLuS, Sina Kissar, and Nader Saedi a/k/a "Turk Server"', Indictment, no date given, p. 5
[12] Ibid.
[13] Violet Blue, 'eBay and PayPal UK domains hacked by Syrian Electronic Army', *ZDNET*, first published 02.02.2014, http://www.zdnet.com/article/ebay-and-paypal-uk-domains-hacked-by-syrian-electronic-army/ last accessed on 16.06.2017.

enough period of time, cause financial trouble for a business. However, these would seem to be, at this point, a very low risk and it is much more likely that the operation would have been designed to create publicity, as was mentioned in chapter three. Yet again, this shows a way in which states can use cyber offensive operation for economic purposes as they are being used to target payment services.

Targeting Individual or Group of Bank Accounts

States could attempt to use a cyber offensive operation to remove money from individual bank accounts. In this type of operation, a state would target a particular bank account or accounts and, either stop a person from being able to access funds, or aim to remove the money completely. Legally, some states do have the power to freeze accounts and they can do this overtly.[14] However, the difference here is that these operations are done covertly.

There have been a number of attacks that have been linked to states but that have targeted non-state organisations, such as banks, to gather information about who uses accounts in banks. The author has not, as of yet, found any attacks which have actually looked to move beyond the targeting of banks to gather information about accounts they hold but it is possible that, in the future, a state could look to use the information they have gathered to produce a cyber effect which is looking to target individual bank accounts. There were reports in 2014 that Russia had targeted the bank JP Morgan and other financial institutions in thirty counties and had managed to steal around one billon dollars worth of funds.[15] It has been alleged that the activity caused around eighty three million names, addresses and email address to be stolen by what some have linked to the Russian government.[16] For example, *The Guardian* reported that FBI sources had, at the time, linked it directly to the Russian government.[17] However, this attack was later linked to two men Josh Aaron and Anthony Murgio. Despite this, there are still accusations that because these men

[14] For example, see HM Government, 'Criminal Finances Act 2017, Chapter 22', Part One, Section 16, and Part Two, Section 40.
[15] Hayley Richardson, 'Companies 'Must See Cyber Attacks as Inevitable'', *News Week*, first published 16.02.2015, http://www.newsweek.com/companies-must-see-cyber-attacks-inevitable-307111?piano_d=1, last accessed on 17.02.2015.
[16] Dominic Rushe, 'JP Morgan Chase reveals massive data breach affecting 76m households', *The Guardian*, first published 03.10.2014. https://www.theguardian.com/business/2014/oct/02/jp-morgan-76m-households-affected-data-breach last accessed on 24.05.2017
[17] Ibid.

frequently went to Russia, they may still have worked for the Russian government.[18] In addition, there have been states that have alleged links to criminal groups as in the case of Russia.[19] This means that a state could ask a criminal organisation to remove money from an account. However, it must be noted that most banks have a policy that, in most cases, when a fraud is detected, banks will refund the money. This means that there could be no real damage done to individuals in cases where money has been stolen from their account. Nevertheless, if, as in the case of JP Morgan, all of those whose personal information was taken were then used to conduct fraud, it would be difficult for a bank to repay all of the funds.

Although, the author has not been able to find examples of states actually conducting a cyber offensive operation in which money was removed from an account, there have been discussions of conducting such operations. This can be seen in the case of NATOs intervention in Kosovo in 1999. It was argued that one operation that was discussed in the planning stage was the use of a cyber effect operation in which the US would remove funds from the President of Serbia's personal accounts so that he would be persuaded to change his policy.[20] However, this idea was abandoned because the US was unsure whether the operation would be legal.[21] However, the fact that this was seen as an option means that it could be used in the future.

Targeting of individual bank accounts could be a way that states could conduct economic operations against terrorist organisations. This could be done in the same way as above in the sense that a state could look to covertly remove money away from an account that has links to a particular terrorist organisations. However, the author has not found any examples of such operations. The main reason why states may not look to conduct such operations is that, once an operation like this took place, a terrorist would likely close the account or, at the very least, know that they were believed to have terrorist connections. This means that the intelligence that a

[18] Lucinda Shen, '7 things we learned about the frat brothers linked to JPMorgan Hack', *Business Insider*, first published 06.08.2015, http://uk.businessinsider.com/7-things-we-learned-about-the-frat-brothers-linked-to-jp-morgan-hack-2015-8?r=US&IR=T, last accessed on, 06.08.2015.
[19] Mark Galeotti, 'Putin's Hydra: Inside Russia's Intelligence Service', *European Council on Foreign Relations*, ECFR/169, (2016), 1-19, 5.
[20] Gregory L. Vistica, 'Cyberwar and Sabotage', *Newsweek Atlantic Edition*, first published on 31.05.1999 accessed via lexis business and news.
[21] Ibid.

state was able to gain from an account could be lost. Furthermore, they may not need to use a cyber offensive operation to conduct such an operation. This is because banks can be forced, under existing laws, to stop a bank account from operating if there is a terrorist connection. Nevertheless, it could be that states would look to conduct such attacks if the countries in which the banks were operating were unlikely to support an overt method of cutting off funds. In this way, a cyber offensive operation might take place so that a bank account and the finances could be targeted to remove terrorist funding. In addition, these types of operations are likely to take place only when it is felt that all the intelligence has been established. Targeting terrorism is likely to be time consuming, in the fact that it would require a lot of intelligence. This is because states will have to identify the accounts that are being used by terrorist organisations. However, an economic cyber offensive operation in which the targeting of terrorist bank accounts, it could be argued, is possible.

Targeting Business Accounts

It is not just bank accounts that belong to an individual that appear to have or even could be targeted in an economic cyber offensive operation. It also appears that GCHQ had, at the very least, developed the notion of using economic cyber offensive operations to target businesses. This can be seen in the fact that GCHQ argued that one way in which they could target a business was through either stopping or diverting the flow of funds between businesses or targeting economically one particular business. GCHQ stated that the purpose could be either to stop deals or to ruin business relationships.[22] The effects of stopping a deal in this way, it could be argued, are considerable. This could be either to the business or businesses that were affected or even the state but indirectly. This is because a business could face a large penalty from not paying the funds. In addition, the effect that it could have on a state, indirectly, is that it could affect the supply chain through which a commodity or product is created and delivered. This means that if there was a piece of equipment that was important to a state by stopping one company from supplying to another company further up the supply chain could mean that a state could have a product that they needed held up or even stopped from reaching them. The effect that the stopping of funds could have on business relationships would be much the same as above.

[22] Edward Snowden Document, GCHQ, 'SigDev Conference 2012 Cyber Integration: The Art of the Possible', with added notes by NBC News, ca. 2012, p. 9, Snowden Surveillance Archive..

Overall, these effects could even force a company into bankruptcy due to the economic pressure that was applied. In these ways, what this clearly shows is that there are a number of ways in which a economic cyber offensive operation can be conducted.

Stopping a business or banks from working

There have been a number of cases when cyber offensive operations have resulted in a loss of data that has had a major effect. An example of such operations being conducted is through the development of logic bombs. Logic bombers are a type of code that becomes active and destroys data on a company system when a set of circumstances, or commands are met. In 2002 a former employee Roger Duronio of USB, a company involved in the global financial market via the stock market, used such a logic bomb. Although this was not a state attack, this type of operation could be used to target companies. Duronio created a programme that was uploaded via a flash drive. This programme then deleted all of the files and it damaged around 1000 USB computers.[23] The attack cost an estimated three million dollar's worth of damage to USB. This example shows that an attack which looks to destroy access to files can have considerable financial damage to systems.

However, these types of attacks do not just have to target financial organisations to cause economic damage. There have been similar attacks on companies that do not belong to the financial services but targeting them could still have an economic effect on a company. Timothy A. Lloyd in the 1990s developed a logic bomb that targeted the systems of *Omega Engineering Inc*. In this attack, the system that deleted software which was highly important to the company and cost the company more than ten million dollars worth of loss, damaged sales and lost contracts.[24] States may look to use this type of attack against companies if they view them as important to a target state in some way. The point would be to severely damage a company so that they would have to stop operating for a little while. Depending on how successful the operation, it is possible that it could bankrupt a company.

[23] Christopher J. Christie, U.S. Attorney, 'United States Department of Justice U.S. Attorney, District of New Jersey News' December 2013, https://www.justice.gov/archive/usao/nj/Press/files/pdffiles/Older/duro1213rel.pdf, p. 3.
[24] David W. Chen, 'Man Charged With Sabotage Of Computers', *The New York Times*, first published on18.02.1998, http://www.nytimes.com/1998/02/18/nyregion/man-charged-with-sabotage-of-computers.html last accessed on 07.05.2015.

There have been examples in which states have used cyber offensive operations that have produced an economic effect by targeting business. This can be seen in the case of the operation directed against the Las Vegas Sands Corp Casino in America. In this attack, the computers that were involved in the business network were wiped, meaning that they could not function.[25] The actual financial loss to the company is not clear but some have estimated that 40 million dollars, if not more, was needed to recover the data and build a new system.[26] The main reason for this operation, as this author argued in the previous chapter, was to send a political message. However, this clearly shows that wiping data on a computer system is a way that a cyber offensive operation can be conducted to produce an economic affect.

It can be seen that GCHQ have also developed tools that could be used in such a way that if they were introduced into a company, they could produce economic harm. There are ways in which a company's information can be erased. GCHQ have developed tools for conducting such operations. Their SWAMP DONKEY tool could be used 'to find predetermined types of file [sic] and encrypt them on a target's machine'.[27] This then could be used to target types of files on a company's computer system which were important for them to fund a business. In addition, they developed a tool, SUNBLOCK, which has the 'ability to deny functionality to send and receive emails'.[28] The targets that SUNBLOCK and SWAMP DONKEY could be used for are not clear as the document states that both of these tools have target restrictions. However, it is clear that tools like these could be used to conduct cyber offensive operations that target businesses in the hopes of producing an economic effect by stopping a business from working.

The Effects of Hacks

Another way in which a state could seek to conduct economic harm on a company is simply by conducting an offensive operation and making sure it is discovered. This

[25] Tony Capaccio, David Lerman, and Chris Strohm, 'Iran Behind Cyber-Attack on Adelson's Sands Corp. , Clapper Says', *Bloomberg* first published on 26.02.2015 http://www.bloomberg.com/news/articles/2015-02-26/iran-behind-cyber-attack-on-adelson-s-sands-corp-clapper-says, last accessed on 27.02.2015.
[26] Benjamin Elgin and Michael Riley, 'Now at the Sands Casino: An Iranian Hacker in Every Server' *Bloomberg*, first published on 12.12.2014, http://www.bloomberg.com/news/articles/2014-12-11/iranian-hackers-hit-sheldon-adelsons-sands-casino-in-las-vegas, last accessed on 27.03.2015.
[27] Edward Snowden Document, GCHQ, 'JTRIG Tools and Techniques', 05.07.2012, p. 6, Snowden Surveillance Archive.
[28] Ibid., p. 6.

then could lead to the organisation which was attacked to suffer from a lack of confidence and turn away clients. This can be seen in the fact that the attack on the company *TalkTalk* has allegedly cost the company around sixty million pounds and caused *TalkTalk* to lose around one hundred thousand customers.[29] Although this example has not been linked to a state this is a way that economic harm can be produced on a private business. This is because once a cyber offensive operation is known then the company can lose money through a loss of customers and a loss of reputation. Although this might not be the main aim of an operation, it does show a cyber offensive operation could be conducted in which the aim is that the attack is discovered rather than who conducted the attack and the aim would be to create a loss of customers or a loss of reputation.

In addition, it has been argued that the operation directed against *Sony Pictures Entertainment* is another clear example of the effects of having an operation conducted. This can be seen by the fact that it was argued by Sharp that the internal leadership of *Sony* were facing internal crisis and *Sony* lost one of their top executives, Amy Pascal.[30] Further, Sharp argued that *Sony* suffered at least 80 million dollar's worth of damage.[31] This clearly demonstrates the fact that the effects of being targeted in an operation can damage a company economically through its reputation.

Cyber Heist

A further way that states could use cyber offensive operations against financial institutions is through the employment of what has been termed a cyber heist. A cyber heist is conducted by targeting banks' or financial institutions' personal accounts rather than the accounts that they run for their clients. This type of operation has so far only been conducted by criminal organisations or by states for a financial gain. However, this type of operation could be employed by states to conduct an economic cyber offensive operation. This is because, in this type of operation, the state penetrates the banks systems and then transfers money that belongs to the institutions themselves. An example of this type of operation occurred when the *Bangladesh Bank* system was compromised and their online credentials for conducting payment

[29] Sean Farrel, 'TalkTalk counts costs of cyber-attack', *The Guardian*, first published on 02.12.2016, http://www.theguardian.com/business/2016/feb/02/talktalk-cyberattack-costs-customers-leave, last accessed on 03.02.2016.
[30] Sharp, 'Theorizing Cyber Coercion', 915f.
[31] Ibid., 917.

transfers were stolen. In this attack, 80 million dollars were stolen by the criminal organisation that was later linked to North Korea.[32] It could be argued that the purpose of this type of attack, if it was to be conducted by a state, would be to affect a bank or financial institutions and, at the very end of it, would look to bankrupt the organisation. This could have major consequences for a bank or institution, in that they may be forced to cover the money that is taken; or a state could be forced to bail out the bank for the loss that has been suffered. In this way, it can be seen that a cyber heist is another way in which states can use economic cyber offensive operations.

Spreading of information

The spreading of information is a further way in which a cyber offensive operation could be conducted to produce an economic affect on a company or even the value of the Gross Domestic Product of another state. In this operation, a state places fake or misleading information in the public domain which suggests that a company is failing, or perhaps, doing better than they actually are. They will then wait for the value of the stock to fall and possibly cause a company to go bankrupt. A state could also conduct this operation directly against states. This would be conducted by spreading false information about a particular commodity that a state is reliant on and then devaluing or raising the price of this commodity.

To show this is not just a hypothetical, it can be seen that there have been charges against a number of people who have been alleged to have committed these types of operations. Gery Shalon, Joshua Samuel Aaron, and Ziv Orenstein were charged in 2013 with conducting a 'pump and dump' operation in which they used 'deceptive and misleading emails' to inflate the value of certain stocks and increase their value.[33] Although there has been no evidence that there was any help from a state organisation, or that this was conducted on behalf of a state, this clearly shows that cyber offensive operations can create economic damage by spreading false information.

[32] Kaspersky Lab, 'Chasing Lazarus: A Hunt for the Infamous Hackers to Prevent Large Bank Robberies', https://www.kaspersky.com/about/press-releases/2017_chasing-lazarus-a-hunt-for-the-infamous-hackers-to-prevent-large-bank-robberies, 03.04.2017, C.F. Kaspersky labs have stopped short of claiming it was The North Korean Government. Richard Ledgett, Deputy Director of the NSA stated that it may have been, see Reuters Staff 'U.S. may accuse North Korea in Bangladesh cyber heist: WSJ' *Reuters*, first published on 22.03.2017, http://www.reuters.com/article/us-cyber-heist-bangladesh-northkorea-idUSKBN16T2Z3?il%3D0, last accessed on 22.03.2017.

[33] United States District Court Southern District of New York, 'United States of America v Gery Shalon, Joshua Samuel Aaron, Ziz Orenstein, pp. 1-2.

In addition, GCHQ argued that one of the ways in which they would target a business would be that they would leak confidential information via online blogs so that the press, another government, or the general public would pick up on the information. This they would support by posting negative information on appropriate forums online so that people would not use the business.[34] This would mean that, if they stopped the flow of customers to a particular organisation, a loss of income for the business.[35] It would also cause a loss of reputation.[36] Additionally, they could use the same techniques that they created for political operations in which they create a 'victim' blog claiming that because of this company doing or not doing something, there has been damage. It is also possible that they could target a particular forum which has built up a reputation for being honest about the information it provides and then use the blog to send misinformation. This is because GCHQ developed a tool called CHINESE FIRECRACKER which was an 'overt brute login attempts against online forums'.[37] If these tools were launched at the right forums, it may be possible for GCHQ to plant misinformation in these forums that would then spread that the idea that a business or a state's commodity is suffering, causing the value of the company to decrease. There is no evidence that GCHQ have actually conducted such operations. However, by GCHQ developing these tools, it does show that, at the very least, they have the possibility of conducting such operations.

All of the above suggests ways in which a state could conduct cyber offensive operations that produce some level of economic effect. In all of these examples, it is clear that states have a number of ways in which they can employ cyber offensive operations to produce economic harm against both other states and non-state actions like business and even terrorist organisations. Some of these operations can be seen to have actually taken place, while others are ways in which states could use these operations. In all of these ways, it is clear that economic cyber operations can be used by states against other states and non-state actors.

[34] Edward Snowden Document, GCHQ, 'SigDev Conference 2012 Cyber Integration: The Art of the Possible', with added notes by NBC News, ca. 2012, p. 9, Snowden Surveillance Archive.
[35] Ibid., p. 9.
[36] Ibid., p. 9.
[37] Edward Snowden Document, GCHQ, 'JTRIG Tools and Techniques', 05.07.2012, p. 5, Snowden Surveillance Archive.

Traditional Covert Action: Paramilitary

The most violent form of covert action activity is paramilitary. There are many different types of operations that form a part of paramilitary activity. Paramilitary covert action includes the training and support to a resistance force, assassination, and, at its highest levels, the operations that use guerrilla forces to try to remove a ruling party by force, such as the Bay of Pigs in 1961 (see below).

Assassination has been defined as 'the targeting of a named individual, whether during peace or war, in order to remove a national security threat'.[38] Assassination as a tool in covert action is a very contentious term and its use has recently caused there to be a lot of confusion between covert action and other operations. This is because of the fact that the US has used drones that have been armed with missiles that have looked to target terrorists to eliminate them. The issue about whether this is covert action stems from the fact that in many instances, the US has admitted that they are the ones who have conducted these operations. However, Lowenthal argues that, strictly speaking, these are not a covert action because they are a military operation and, at times, have been publicly confirmed. In addition, when the British first used their own drone to conduct an assassination, the British classed this as an act of war rather than covert action. This can be seen from the fact that when the British used a UAV to kill Reyaad Khan, they sent a letter to the United Nations Security Council stating this operation was launched under an article 51 of the UN Charter.[39] These operations have been referred to as targeted killing because they have been used as an act of war rather than covert action.[40]

However, it could increasingly be that UAVs could, in the future, be controlled by intelligence agencies to conduct assassinations. Even if the use of UAVs to conduct assassinations as part of covert action is at this point unclear, this does not mean that assassination has not been used as a tool of covert action. It was argued by Richelson that the US had under the CIA around eight different plots to conduct

[38] Jeffrey T. Richelson, 'When Kindness Fails: Assassination as a National Security Option', *International Journal of Intelligence and CounterIntelligence*, 15:2, (2002), 243-274, 245.
[39] United Nations Security Council, 'Letter dated 7 September 2015 from the Permanent Representative of the United Kingdom of Great Britain and Northern Ireland to the United Nations addressed to the President of the Security Council' http://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_2015_688.pdf
[40] Lowenthal, *Intelligence*, Seventh Edition, p. 269.

assassination in 1960-1965 against the Cuban leader, Fidel Castro.[41] There are many ways that states have conducted assassination covert actions.

Sometimes it has been claimed that, rather than one state conducting assassination, there have been attempts by states to get others to conduct the assassinations on their behalf. This can be seen in the US involvement in the Congo. Through the US' involvement under the CIA in the Congo, it has been claimed that the CIA had intended to assassinate the former Premier and opposition leader, Patrice Lumumba. Some CIA officers were reported to have asked for the 'permanent removal of Lumumba'. The reason that the US felt the need to kill Lumumba was that when he was involved in the independence of the Congo from Belgium, he had become increasing involved with the Soviet Union. This meant, in the US's eyes, that he was a threat. This even extended to when he was removed from office and he still had a lot of support. Although this operation appears to have been just encouragement rather than supplying of materials that were used in the assassination, the US had looked at ways in which they could supply the help needed for the assassination attempts.[42] In this way, although the CIA did not conduct the assassination, they could be seen to be in some way actively involved in the operation. This has not been the only time in which the US has tried to use other groups to conduct assassination attempts. In Cuba, the US wanted to use the criminal underworld to help them assassinate Fidel Castro.[43] This was not the only attempt and plan that the US had to try and kill Fidel Castro but it does show that states can look to use others to conduct assassination for them. In these ways, a form of covert action is using other groups to conduct assassinations on a state's behalf.

A further way that states can conduct paramilitary covert action is through directly helping terrorist or guerrilla organisations in the hopes that this would destabilise the government of the target state.[44] There have been many ways and reasons for conducting such operations. One of the reasons can be that there is a state that another state is hoping to undermine. This type of operation can be extremely

[41] Richelson, 'When Kindness Fails', 247.
[42] United States, Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, 'Alleged Assassination Plots Involving Foreign Leaders: An Interim Report Of The Select Committee To Study Governmental Operations With Respect To Intelligence Activities United States Senate Together With Additional, Supplemental, And Separate Views', pp. 17-19.
[43] Ibid., p. 74.
[44] Godson, *Dirty Tricks and Trump Cards*, pp. 161-170.

helpful, when it is known that the target of the operation, which is in most cases, although not always, another state, then the state that is conducting the operation, can help the terrorist or guerrilla organisation so that they could target the other state. At times, all that is needed is a small token level of support that is designed to show that a particular government supports you. This can be seen in the CIA activities in Chile in 1970 in which they provided just three weapons to a group who were preparing to partake in a military coup. In addition, the operations do not even need to be weapons. Sometimes, as in the case of CIA's involvement in Guatemala in 1952-1954 the operations can be much bigger. The CIA aimed to give enemies of the communist government in October 1952 around '250 rifles, 380 pistols, 64 machine guns and 4500 grenades'.[45] The levels can increase and it is possible that states can look to get weapons from one source so that they can be given to others. This can be seen in the fact that the US looked to persuade Egypt and China to sell guns to the Mujahidin fighting the Soviet Union in Afghanistan.[46] This was noted by Roy Godson who argued the support that is given does not have to be military, but could instead of just be giving military equipment. Groups can be given intelligence about the government which they are trying to overthrow, or, if it is possible, they could receive intelligence about various aspects of the population that would help the guerrilla forces to gather support across the country.

In addition to helping a guerrilla force, states can also use their own powers to help bring their ideas to the world's attention and help demonise the government they are fighting. This was particularly useful in Afghanistan where both the British and the Americans were able to show enemy atrocities and then use this to gather more help during the 1980s.[47] Sometimes, the support that these organisations need is a safe haven from where they can operate, train, and get support of the local population. There are many examples of where this has been important. For example, with the support of Honduras and Costa Rica, the Contras, who were supported by the US and attempted to overthrow the government in Nicaragua, were able to increase their size from ten to fifteen thousand. This shows the effectiveness of providing a safe haven for groups to operate in, as it allows these groups to mass and over time gather

[45] Cullather, *Secret History*, Second Edition, p. 29f
[46] John Prados, *Presidents' Secret Wars CIA and the Pentagon Covert Operations From World War II through the Persian Gulf*, Revised and Expanded Edition (Chicago: Elephant Paperback, 1996), p. 359.
[47] Godson, *Dirty Tricks or Trump Cards*, p. 167.

support in a place where they are harder for government that is targeted to get to them and thus stop the operation from happening.[48]

It can also be seen that the British even used such methods against non-state actors as well. In the late 1980s, the Security Service conducted a campaign in which they provided intelligence about the PIRA to the general public about the people who the members of the PIRA. [49] However, it must be noted that this operation in a review was seen as propaganda and does appear to have been designed to have been solely a propaganda campaign.[50] Nevertheless, although a review into this operation saw it as propaganda, it also acknowledged that it does come close to something else. One of the MI5 officers involved in this campaign stated that it was designed in such a way that '"challenges republican assertions, which makes republican players feel that they, too, are as exposed as the members of the security forces who live daily under threat of the assassin's bomb or bullet"'.[51] This would then make it appear that it could be something more than propaganda as it is more aggressive in its objective. Whether this particular operation could be seen as something more than a propaganda campaign is to some extent irrelevant. This is because what this case does show is a way in which a government could conduct a covert action operation against a particular terrorist or guerrilla movement. This is because a state would be providing details about a particular terrorist organisation when it knows that there is a violent rivalry in the country in the hopes that another organisation would target a particular individual. This would then mean that a rival organisation could then target for attack, kill or even target the family of those whose who were identified.

The most widely known example of paramilitary covert action was the Bay of Pigs operation in 1961. The Bay of Pigs was an operation in which the CIA had trained, supplied weapons to and helped land around 1,400 Cuban exiles. These Cuban exiles, it was hoped, would create an insurgency that would overthrow the Cuban government who were viewed as communist and remove the leader of Cuba, Fidel Castro.[52] It is at this point that the use of covert action comes closest to being an

[48] Ibid., p. 170.
[49] Desmond de Silva 'The Report of the Patrick Finucane Review Volume I' December 2012, (London: The Stationary Office, 2012), p. 297
[50] Ibid., p. 297
[51] Ibid., p. 297
[52] Bevan Sewell, 'The Pragmatic Face of the Covert Idealist: The Role of Allen Dulles in US Policy Discussions on Latin America, 1953–61', *Intelligence and National Security*, 26:2-3, (2011), 269-290, 288.

act of war. However, the difference is again, that covert action is chosen for this type of operation as states are wishing to maintain the ability, however, flimsily, to argue that they were not the ones to have conducted the operation. There are many different types of operations that form parts of paramilitary operations. They cover training and support to a resistance force, assassination, and support for guerrilla forces, to their highest level where it tries to use force to remove someone power, such as the Bay of Pigs.

In these ways, paramilitary operations are the most aggressive form of covert action. They are also seen as type of activity that is most likely to allow for a state to lose plausible deniably. The use of such activities is where covert action blurs the line between actions taken in peace and an act of war. This is due to the violence. The Bay of Pigs, and the actions in Nicaragua are very much akin to an act of war. This is because a state has come close to reaching the level of threat necessary for a state to have a claim of an act of war.

High-End Cyber Offensive Operations

High-end cyber offensive operations are used to produce the highest level of aggression. They can be targeted against states, non-states actors such as businesses, or they can be used against terrorist organisations. These operations cause the most damage such as stopping a power station from work and even, it is possible, death if the right form of activity takes place. These high-end operations are made up of four forms of operations. There are individual operations, affecting government systems, cyber assassination, and, finally, targeting critical national infrastructure.

Individual Operations

The first type of high-end cyber offensive operations are those that have the ability to stop an individual from working. Although these operations could be used against anyone, this author believes that these types of activities are high-end operations because it is the author's opinion that techniques such as these would be reserved for those who are very important to a state or an organisation. This is because once methods such as these are used against a person or people, other states and organisations will look to access how the operation was conducted and then look for ways to stop it from happening to themselves or others. This means that it will likely

only be used against those who are important. In this way, these types of cyber offensive operations should be seen a high-end operation.

Much as with other operations, there are a number of ways in which these tools could be used. It is clear from Snowden's files that GCHQ has this ability. One of the most aggressive tools that was listed on JTRIG file was called ANGRY PIRATE. ANGRY PIRATE has the listed ability of allowing it to stop someone from having access to his or her computer.[53] This tool, however, was restricted. This, it could be argued, means that this tool was likely reserved for only use on high level targets. This means that it would allow a country to complete shut off what this person could do.[54] A further tool with a similar ability to ANGRY PIRATE was AMBASSADOR'S RECEPTION. AMBASSADOR'S RECEPTION is a virus that has the ability to 'encrypt itself, delete all emails, encrypt all files, make the screen shake and no more log on'.[55] Further, GCHQ created a tool termed SILENT MOVIE. SILENT MOVIE is a tool that was designed to produce a denial of service attack against people who are using Secure Shell service (SSH).[56] SSH is a way in which people remotely login to networks over unsecured systems. This means that if a person who works for a government requires remote access to allow them to work, they will be stopped from working. What this means is that these tools have the ability to stop someone from doing their job.

By using these tools against a select person, a state could produce damaging effects against another state or a terrorist organisation. For example, if these systems were used against the IT administrator for an organisation, then they could use this to affect this administrator from being able to access a system. It could be used against a state, by targeting someone with a significant role within a state in such a way that it limits their ability to respond to a situation or problem. This could be used against non-state actors like businesses and used in conjunction with other operations to limit a person's ability to stop the attack. Further, while terrorist organisations such as IS have made use of the Internet to recruit and plan attacks, if a intelligence organisation discovered the main person or people who were conducting these activities for IS,

[53] Ibid., p. 5.
[54] Ibid., p. 5.
[55] Edward Snowden Document, GCHQ, 'SigDev Conference 2012 Cyber Integration: The Art of the Possible' with more information added by NBC News, ca. 2012, p. 12, Snowden Surveillance Archive.
[56] Edward Snowden Document, GCHQ, 'JTRIG Tools and Techniques', 05.07.2012, p. 6, Snowden Surveillance Archive.

shutting down this person's access could damage IS or other terrorist groups. In these ways, it is clear that targeting an individual's access to a system could have highly damaging effects.

Stopping Government or Organisations Systems from Working

A further way in which high-end operations can be conducted is through operations that are designed for stopping government or organisations from working. These operations are similar to the operations that were discussed in the previous chapter under political target for retaliation. However, the key difference is a state is directly targeting systems that are connected to the government. As such, these activities are of higher violence than targeting businesses. One way would be for states to get into an organisation that works directly for a state and stop them from being able to function. One example of such activity would be the ability of states to develop tools that follow the pattern of Ransomware that encrypts systems that are linked to a state such as the Ramsonware operation termed WannaCry.[57] Although in this case, it appears that this was state sponsored and the fact that it actually targeted a British government institution, the NHS, it has been noted that it does not appear that the NHS was actually a direct target.[58] It appears that the targeting of the NHS and encrypting the systems was an accident. However, it can be argued that if an operation was conducted in which systems were encrypted that a government needs, then a considerable amount of damage could be done directly against a state.

There is clear evidence that the use of cyber offensive operations that stop an organisation from working has been used against non-state actors. This can be seen in the fact that in April 2016, it was stated that US Cyber Command had begun to launch cyber offensive operations against IS. It was stated that these operations were designed to target the group's command-control and communications.[59] It appears that one of the aims of this operation was to stop terrorist organisations from being able to communicate with their people via the Internet.[60] How, exactly, the US conducted this operation remains unclear. It also appears that much of the operation

[57] Gordon Corera, 'NHS cyber-attack was 'launched from North Korea'', *BBC News,* first published on 16.06.2017, http://www.bbc.co.uk/news/technology-40297493, last accessed on 16.06.2017
[58] Ibid.
[59] Shane Harris and Nancy A. Youssef, 'U.S. Ratchets Up Cyber Attacks on ISIS', *The Daily Beast,* first published on 18.04.2016, http://www.thedailybeast.com/articles/2016/04/17/u-s-ratchets-up-cyber-attacks-on-isis.html?via=desktop&source=twitter, last accessed on 18.04.2016.
[60] Ibid.

seems to be directed towards intelligence gathering about IS but because of the fact that US Cyber Command was aimed at stopping terrorist organisations from being able to communicate that a cyber offensive operation was launched to affect IS. In addition to US Cyber Command it can be seen that GCHQ have also developed tools that could be used for similar operations to those conducted by US Cyber Command against IS. This includes AMBASSADORS RECEPTION that was discussed above.[61] In addition to AMBASSADORS RECEPTION, GCHQ developed two other tools. One was termed ANGRY PIRATE, which permanently disables a target's account on their computer, and the second termed SUNBLOCK that stops the sending of emails or material online. In addition, they have developed tools that target phones by sending a number of phone calls to a number so that they cannot communicate via this. In this way, states have the ability to stop terrorist organisations from functioning. If these tools could be directed towards a terrorist organisation, they could allow for the organisation to collapse.

Assassinations

The use of cyber offensive operations to conduct assassinations has not happened yet. This means the threat is hypothetical. Nevertheless, there is a threat that a state may use high-end cyber offensive operations to conduct an assassination. The Department of Defense listed one of the threats that they face is that a group could gain access into health systems and change medical history.[62] Furthermore, there is a danger that as so many systems are connected to the Internet in some way, systems for critical life support devices could be altered. It was reported in 2013 that a hardcoded password was programmed into a system that linked to a number of medical devices. These included 'surgical and anaesthesia devices, ventilators, drug infusion pumps, external defibrillators, patient monitors, and laboratory and analysis equipment'.[63] Some of these devices, using the hardcoded password, allowed for a person to change settings. If this happened, it could cause a hospital patient to be killed. While this particular case did not actually see anyone harmed by the use of a cyber offensive operation, it

[61] Edward Snowden Document, GCHQ, 'JTRIG Tools and Techniques', 05.07.2012, p. 5f, Snowden Surveillance Archive.
[62] US Government, The Department of Defense, 'The Department of Defense Cyber Strategy', April 2015, p. 2.
[63] US Government, ICS-CERT Alert (ICS-ALERT-13-164-01), Medical Devices Hard-Coded Passwords, https://ics-cert.us-cert.gov/alerts/ICS-ALERT-13-164-01, first published, 13.06.2013, last accessed 16.01.2017.

does show that cyber offensive operations could be used to conduct assassinations. Furthermore, Barnaby Jack, a cyber security researcher was believed to have developed, just before he died, a way in which a pacemaker could remotely effected, causing it to kill the person who uses it.[64] The danger that this presents towards a state is that if a head of state was to need a medical device to keep them alive then it is theoretically possible that a state could use this kill them.

Although it is theoretically possible that states could look to conduct a cyber assassination in the ways mentioned above against terrorist organisations, it must be noted that this is unlikely. This is because, at the moment, at least, they do not have any need to conduct operations like this. As in the case of the targeting of IS and Al Qaeda, states have the ability to conduct air bombing campaigns in various ways, including drones. This means that they currently have no need to use cyber offensive operations to conduct assassinations. It is likely that they would choose this method over cyber operations as they are easier. Until this changes, there are unlikely to be any attempts to use cyber offensive operations to conduct assassinations against terrorist organisations.

Cyber assassination operations are likely to be very rare, in contrast to the frequency with which they take place in films and television shows. There are simpler ways for states to conduct assassinations than using these operations. It is likely that this type of activity would only be directed against a highly important individual. This means that the damage that is likely to come from these types of operations is likely to be high. In addition, these types of operations will take a long time to plan. This means that the ability to access a system that a person could use could be improved. In these ways although it is theoretically possible to use a cyber offensive operation to assassinate someone, there are problems in conducting these operations.

Targeting Critical National Infrastructure

The targeting of critical infrastructure is a problematic type of operation. This is because the targeting of a power grid is likely to be of such a high level of threat, that, as was referred to by Freedman, that an act war may be reached.[65] However, it is clear that there have been cases where governments have planned to conduct these types of

[64] Jeremy Kirk, 'Pacemaker Hack can deliver deadly 830 volt jolt', *Computerworld*, first published 17.10.2012, https://www.computerworld.com/article/2492453/malware-vulnerabilities/pacemaker-hack-can-deliver-deadly-830-volt-jolt.html last accessed 16.01.2017.
[65] Freedman, 'General Introduction', p. 1.

operation. This is because the Snowden documents show a spectrum of effects that have been considered (see figure three), with the highest being targeting national infrastructure.

However, the targeting of critical national infrastructure can be seen to have taken place. The UK defines critical national infrastructure as chemicals, civil nuclear communications, defence, emergency services, energy, finance, food, government, health, space, transport and water.[66] In the US, it is counted as chemical, commercial, communications, critical sector management, dams, defence, emergency services, energy, financial, food and agriculture, government, health, Information technology, nuclear, transportation, water and waste management.[67] If cyber offensive operations were used by a state to directly affect and disrupt these services, this would be the highest level of operation. There have been a number of authors who have shown the ways that these targets are possible. In addition, there have been several cases in which private individuals, who have worked in these sectors for businesses, have become disgruntled and launched an attack.[68] However, until recently, there had not been a confirmed attack in which a critical national infrastructure had actually been directly targeted by a state against another state.

An alleged example of such an operation took place and appears to have been conducted by the US was in December 2014 when the entire Internet access of North Korea was taken down. In this attack, the Internet of North Korea was completely shut off inside North Korea for around ten hours between 21 and 22 of December 2014. Although it is not clear who conducted this operation, it has been alleged that it was US government. A Republican Congressman, Michael McCaul of Texas, stated that it was an operation conducted by the US because of the activities of North Korea against the film industry.[69] However, there are conflicting accounts about whether the US actually launched the operations. Fred Kaplan, has stated that the US government were not involved in the attack which took away North Korean Internet access.[70] It

[66] UK Government, Centre for the Protection of National Infrastucture, https://www.cpni.gov.uk/critical-national-infrastructure-0, last accessed on 16.02.2015.
[67] US Government, Department of Homeland Security, 'Critical Infrastructure Sectors' https://www.dhs.gov/critical-infrastructure-sectors
[68] On the disgruntled employee see Rid, *Cyber War Will Not Take Place*, pp. 72-79
[69] Chris Strohm, 'North Korea Web Outage Response to Sony Hack, Lawmaker Says', *Bloomberg*, first published on 17.03.2015, http://www.bloomberg.com/politics/articles/2015-03-17/north-korea-web-outage-was-response-to-sony-hack-lawmaker-says, last accessed on 19.03.2015.
[70] Kaplan, *Dark Territory*, p. 271.

does seem that Congressman Michael McCaul was unlikely to know if it was the US government that conducted the operation as he was not a member of the House Permanent Select Committee of Intelligence although he was chairman of the House Committee on Homeland Security at the time. However, what is clear is that North Korea's access to the Internet was taken completely offline.[71] There are a number of implications arising from this attack. In the attack, the number of Internet Protocols (IP) addressed inside North Korea was 1024.[72] This means that there was only a small population of North Korea that was connected to the Internet. North Korea lost all access to the Internet for ten hours. Even if this was not conducted by the US, or even any state, the ability of a state to shut off the Internet could have damaging effects on a state. It could affect the ability of states to communicate domestically or internationally. However, it must be noted that it is difficult to conduct such operations. In North Korea, with only a few systems connected to the Internet, it was possible. For a country with more Internet connections, it would be harder to conduct an operation to take down all Internet access. However, this type of operation is possible and, in this way, the ability of a state to completely shut off the Internet of another state must be seen as a form of cyber offensive operations.

One of, if not the best known, example of states using cyber offensive operations to conduct a high-end operation was the Stuxnet operation against the Iranian nuclear programme based in Natanz that was discovered in 2010.[73] The Stuxnet programme gained access to the Iranian systems. Although the worm spread through many different countries, it was noted by Symantec that the main geographical place that the Stuxnet was uncovered was Iran, indicating that it was targeting Iran.[74] It was also noted that it was a complex system that contained four zero day attacks and it faked two digital certificates which indicate a state or states' involvement in the operation.[75] A zero day attack is a term for a previously unknown issue within software. Stuxnet was also designed in such a way that it prerecorded data about the system that it would later use.[76] Stuxnet changed the Programmable

[71] Ibid., p. 271.
[72] Ibid., p. 271.
[73] C.F. Stuxnet is the worms most common name however it is noted that it was actually part of a cyber offensive operation code named Olympic Games.
[74] Nicolas Falliere, Liam O Murchu, and Eric Chien, 'W32.Stuxnet Dossier Version 1.4' (February 2011) *Symantec Security Response*, p. 3
[75] Ibid., p. 3
[76] Rid, *Cyber War Will Not Take Place*, p. 44.

Logic Controller. It was designed to affect the way that the nuclear centrifuges worked. This was achieved by changing the speed of the spinning centrifuge causing it to speed up and slow down.[77] This then would cause the centrifuges to break. Stuxnet also made sure that, at the same time, it reported back to the system that everything was operating normally.

However, judging the effectiveness of the Stuxnet operation can be difficult. It was argued by Ivanka Barzashka that the real success of this operation was minimal.[78] This argument was further supported by Jon Lindsay, who has pointed out that although Stuxnet caused damage to around 11.5 per cent of the centrifuges, the normal breakage of these centrifuges was around 10 per cent anyway.[79] Further, it was felt by US officials that they only delayed the development of Iranian nuclear weapons by around eighteen to twenty four mouths.[80] However, this may have been the actual intention because of the design of the operation. It could have been that an operation using very similar techniques could have been designed that would have meant that the affects were more damaging. This would, however have been more obvious and people would have begun to investigate. It would make sense that if a state was looking to try and affect another state's ability to create a nuclear weapon, that it would want to make sure that the operation could continue to function over a longer period of time but be less obvious. Furthermore, by designing it to be less obvious it may have also meant that the Iranians believed that the issue was caused by other things rather than a state affecting their systems. Such a situation may have been that by slowing down the Iranian nuclear scientists in creating the nuclear material, even if it was only by a small amount, the scientists may have been fired from the project. This would then further affect the Iranian nuclear program. This would mean that a state would want to make sure it had some effect but not so much that the target state look too hard at their system. The operation could have been operating a lot longer due to the way that it was only to have a marginal effect rather than a more noticeable effect had it not jumped outside of the Natanz network.[81] It was noted that

[77] James P. Farwell and Rafal Rohozinski, 'Stuxnet and the Future of Cyber War', *Survival*, 53:1, (2011), 23-40, 29.
[78] Ivanka Barzashka, 'Are Cyber-Weapons Effective?', *The RUSI Journal*, 158:2, (2013), 48-56, 48.
[79] Jon R. Lindsay, 'Stuxnet and the Limits of Cyber Warfare', *Security Studies*, 22:3, (2013), 365-404, 391.
[80] Zetter, *Countdown to Zero*, p. 360.
[81] Kaplan, *Dark Territory*,

because of the sanctions against Iran and with Iran losing centrifuges due to normal wear and tear, if Stuxnet had not been discovered, it could have had a bigger effect.

Finally, it was noted if there had been a massive sudden sabotage, this would have increased the risk of retaliation.[82] This means that if it became visible to others, it would have been disclosed. This was noted in a file produced by GCHQ subtle effects that could be used for long-term operations. [83] This is what Stuxnet appears to have been designed for. An operation such as this would be likely to plan to damage only a small part of the process. This could be done by changing the programme code for a piece of equipment so that it changes what the equipment does which causes a system to stop working. However, one way that cyber offensive powers could be used is to change orders of equipment on outside sources. Although it is not clear if an operation such as this has taken place, it would allow for a way to effect an operation in a way that is not easy to track. In this way, it is clear that this type of operation does have the ability to stop something from working and that if this was used to stop a government from achieving an objective, then this would be a high-end use of cyber offensive operations.

In 2015, it can be seen that a cyber offensive operation was conducted that directly affected the functioning of a power plant. This was the BlackEnergy3 virus. The original BlackEnergy virus appears to have been created as a simple DoS system.[84] On the 23 of December 2015, approximately 225,000 people in the Ukraine were left without power as the virus targeted three of the power electrical distributors.[85] This appears to have been caused by the virus taking control of the substation breakers and leaving them open.[86] It has also been reported that part of the virus contained a killdisk function that wiped the data. [87] This meant that it was harder

[82] Zetter, *Countdown to* Zero, p. 365.
[83] Edward Snowden Document, GCHQ, 'SigDev Conference 2012 Cyber Integration: The Art of the Possible' with added notes by NBC News', ca. 2012, p. 14, Snowden Surveillance Archive.
[84] Raj Samani and Christiaan Beek, 'Updated BlackEnergy Trojan Grows More Powerful', *McAfee*, 14.01.2016.
[85] US Government, Department of Homeland Security, 'Industrial Control Systems Cyber Emergency Response Team Alert (IR-ALERT-H-16-056-01) Cyber-Attack Against Ukrainian Critical Infrastructure'
https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01, first published on 25.02.2016, last accessed on 25.02.2015.
[86] Gaoqi Liang, Steven R. Weller, Junhua Zhao, Fengji Luo, Zhao Yang Dong, 'The 2015 Ukraine Blackout: Implications for False Data Injection Attacks', *IEEE Transactions on Power Systems*, 32:4, (2017), 3317-3318, 3317.
[87] Department of Homeland Security, 'Industrial Control Systems Cyber Emergency Response Team Alert (IR-ALERT-H-16-056-01) Cyber-Attack Against Ukrainian Critical Infrastructure'

for the system to become operational even once people realised that the operation was taking place. Further, it has been alleged that virus was also coordinated with operations against the telephone systems of the engineers of the power plant to create an even longer delay in being able to report the problem or get engineers out. [88]

It must be noted that there has not been, as of yet, any public announcement identifying the perpetrators of the operation. *McAfee* has stated that, although it could well be a state sponsored operation, they do not have the ability to state this at this point. However, due to the ongoing issues in the Ukraine with Russia around the Crimea, it would seem plausible that it could have been them. This is because it has been noted that BlackEnergy3 needed a lot of reconnaissance for the operation to succeed. In addition, with the virus appearing to be designed to increase the difficulties of restoring power, this further adds to the speculation that it was part of a Russia's operations against the Ukraine. However, this is not conclusive. This event is so significant because it could have been the first time that a cyber offensive operation that was state sponsored had ever taken down a power plant. In addition, the fact that the operation was conducted in the winter would further show its potential effectiveness to damage and change the Ukrainian government's policy towards Russia and the Crimea.

Nevertheless, this is not the only way that another state could affect a state's ability to have power. Russia has a long history of using its gas and oil supplies to try and force other states to change policy.[89] The difference is that this would have been done in such a way that it would have caused the Ukrainians to suspect but not know completely if it was actually the Russians. Further, this operation is a perfect statement of fact towards the US and its allies. The confrontation between the Ukraine and Russia over control of the Crimea was still on going at this point, and there has always been speculation that the US would send in more support to the Ukraine. By conducting the operation, it could force the US and its allies to change their policy towards the Ukraine for fearing a similar activity being conducted against them.

---

https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01, first published on 25.02.2016, last accessed on 25.02.2015.

[88] Liang, Weller, Zhao, Luo, Dong, 'The 2015 Ukraine Blackout', 3317.

[89] Mark Galeotti, 'Hybrid, Ambiguous, and Non-linear? How New is Russia's 'New Way of War'?', *Small Wars & Insurgencies*, 27:2, (2016), 282-301, 286.

In addition to the Black Energy Virus, there was another operation that targeted Ukrainian power supplies in 2016. It was fully automated, whereas the BlackEnergy3 malware needed someone to provide more information, CRASH OVERRIDE or Industroyer, did not as it was able to do this via an automated process and could even be timed to take effect later.[90] The actual effect of the malware was limited to parts of Kiev that were only without power for around an hour. It has been alleged that this system could be used on many other networks. It was further argued that this type of operation could have been used against other systems including Europe, the Middle East, Asia, and with a little modification the US as well.

However, a point needs to be highlighted here. It is still a lot easier for states to conduct other types of operations to affect the power supplies of another state than it is to use cyber tools. It was noted that in the US by causing a large-scale power outage, six people could destroy six substations using bombs or means other than cyber. It is likely that this would, in reality, be more damaging. Further, animals affect the systems far more commonly cause power outages. Yet, what the operation does show is that states do have the ability to use cyber offensive operations that target national infrastructure and cause problems. It is likely, as was stated above, that this was as much about getting the Ukraine or their allies to change a behaviour but not in such a way that it would become obvious.

It is also argued that damaging or affecting a system does not just have to come from affecting a computer system the way Stuxnet did. States may have the ability to affect a system by using deception. It was argued that such an operation took place and that it was used to destroy an oil pipeline in Russia. This was argued in the 1980s with America conducting such an operation. In the 1970s, the CIA gained access to a double agent, Vladimir Vetrov, codenamed FAREWELL. They discovered that the Soviet Union were looking at stealing some automated pumps and valves control systems from Canada. When the CIA discovered this, then allegedly affected the systems so that at first, they would work and later, they would destroy themselves.[91] This caused the pipeline to explode.[92] However, there is very little evidence to suggest that this operation actually took place. Two books authored by

[90] Andy Greenberg, ‘‘Crash Override’: The Malware That Took Down A Power Grid’ *Wired*, first published 12.06.2017, https://www.wired.com/story/crash-override-malware/, last accessed on 12.06.2017.
[91] Clarke and Knake, *Cyber War*, p. 93.
[92] Clarke and Knake, *Cyber* War, p. 93.

Christopher Andrew and former KGB officers only seem to indicate that FAREWELL was used for counter intelligence purposes.[93] In addition, Douglas Porch who conducted a study of the French intelligence services who FAREWELL originally worked for as a double agent, found no evidence of such an operation.[94] Finally, it was argued by Gordon Corera that after speaking with classified sources who would have been in the know about such an operation, there was still no evidence of such an operation taking place.[95] Nevertheless, even if this operation did not actually take place, it could be argued that an operation could be conducted which is similar but it would be very difficult to achieve. In this way, although this operation may not have happened, it is clear that such an operation could happen.

In terms of the high-end cyber offensive operations that have been looked at such as individual disruption, assassination and targeting of critical national infrastructure; are not unlikely to take place too often. This is because the threats that these pose if they are discovered are huge. The threat can either be technical, in the sense that once an operation like this is discovered, then states are going to begin to look at how the operation was conducted and come up with ways to stop them from happening in the future. A further reason that operations like this are likely to be limited is that a state's political reputation can be affected if they are discovered. Finally, these types of operations, if a state conducted them, would be within the realms of an act of war as was stated in the first chapter due to the level of threat of the activity. Although this argument can relate to all forms of cyber offensive powers, it must be noted that the higher the level of aggression, the more likely it is that the need to track it back to another state will happen. This is because attributing which group or state committed a cyber operation can be a long process. Because it can be a long process, it means that it is likely that it will only really be done when the operation is at the higher end. This means, as was stated before, states will be unlikely to use high-end cyber unless it is absolutely necessary.

---

[93] Christopher Andrew and Oleg Gordievsky, *KGB: The Inside Story of its Foreign Operations from Lenin to Gorbachev* (London: Hodder & Stoughton 1990), p. 522, and Andrew and Mitrokhin, *The Mitrokhin Archive* (London: Penguin 2000), p. 619f.
[94] Douglas Porch, *The French Secret Services: From The Dreyfus Affair to the Gulf War* (Oxford: Oxford University Press, 1997), p. 447f.
[95] Corera, *Intercept*, p. 150f

Comparison

Having established how economic and paramilitary operations have been seen to be a form of covert action in the past it is clear that there is a direct connection between these two activities and cyber offensive operations.

Firstly, both traditional covert action and cyber offensive operations have been targeted via economic operations and paramilitary operations against state actors and non-state actors. From this, the fact that cyber offensive operations have been used to target non-state actors does not mean that they cannot be seen to have a direct connection with covert action in terms of who they have been used against.

Secondly, there is also evidence much the same as with propaganda and political activities which had operations that can be seen to have taken place in both accounts. This can be seen in economic operations in which states have used false information to affect the economic outputs in traditional covert action. This was demonstrated to have a use in cyber offensive operations as well. In terms of paramilitary operations it can be seen that high-end cyber offensive operations offer the ability, although at this point it is only theoretical for states to use these tools to conduct assassinations.

In terms of economic operations, the fact that states have used a number of new tools to target adversaries that have not been seen to have taken place with traditional covert action does not mean that there is not a direct connection between cyber offensive operations and covert action. This merely means that states have adapted to the new ways to target adversaries to produce an economic effect. Overall therefore, it must be seen that in terms of economic operations, a direct connection between covert action and cyber offensive operations exists and that they are on balance the same type of activity.

In terms of high-end cyber offensive operations and paramilitary operations there is a connection. In 2017 Lowenthal argued, that cyber offensive operations could achieve sabotage operations.[96] This is what this author has referred to as targeting of critical national infrastructure. This author would argue that the inclusion of sabotage is flawed. The reason that these operations are directly connected to paramilitary operations is because if a state trained a guerrilla force to destroy another

[96] Lowenthal, *Intelligence*, Seventh Edition, p. 256f.

state's power system, these would be termed a paramilitary operation. These operations would also be termed a paramilitary operation if a state used their own intelligence agency to conduct a similar operation. From this, high-end cyber offensive operations should be seen as the cyber means equivalent of paramilitary operations.

The fact that high-end operations offer different ways to conduct operations to paramilitary activities does not mean that they are not directly connected. The fact is that states will and have attempted to use new technology to attempt to affect other states. This can most clearly be seen in assassinations. In terms of when the historical research on the use of assassinations as being covert action was first thought of states did not have access to drones. States using drones to conduct assassinations did not change the fact that assassinations were not a form of covert action. It was just that states were using a new technology to conduct a paramilitary operation. From this therefore the argument must be simply because states are using a new form of technology did not change the fact that this is a form of covert action.

In all of these ways it is clear that covert action and cyber offensive operations have a direct connection between one and other in terms of economic and paramilitary operations.

Conclusion

The first purpose of this chapter was to argue that it can be seen that there is a direct connection between covert action and cyber offensive operations in terms of economic and paramilitary operations. To do this, it first had to demonstrate the use of these types of covert action and then establish if states have used these types of activities as part of cyber offensive operations.

This chapter has argued that states could use their cyber offensive operations to conduct economic operations to produce an economic effect on a business or a state. These types of operations could include conducting a DDoS attack against a bank. This would have the effect of stopping clients from accessing banking systems. States could use cyber offensive operations to target personal or business accounts. These could be used to freeze accounts or even remove money completely. They could also release information that would affect the value of a particular commodity

or even destroy the reputation of a business. States could also use the technique of cyber heist where they take money directly from the bank's network. States could also use operations that directly target stock exchanges. However, this, the chapter has argued, is unlikely because all states are likely to become affected by that.

This chapter has also argued the use of cyber offensive operations to conduct high-end operations. These operations are designed to affect a system or stop it from working. This includes stopping individuals from have access to systems. This chapter has argued that this is a high-level operation, as it would most likely be targeted at someone who is important to either a terrorist organisation or a government. It has also argued that states have many ways in which they can use operations that are designed to stop government systems and terrorist organisations from being able to work. This includes encrypting data on a system's computer. It has also argued that, although cyber assassination has not happened yet, there is a chance that, in the future, an operation could be conducted in which states use cyber offensive operations to kill people. Finally, it has argued that the highest level of operations which states can use against other states and non-state actors are operations that effect the ability of critical national infrastructure from functioning. This includes shutting off power to a state. In these ways, this chapter has demonstrated two of the ways states can use cyber offensive operations.

Using the fact that it can be seen that states have used cyber offensive operations for economic and high-end operations, the chapter then looked to conduct a comparison between these activities and covert action. This chapter has argued that cyber offensive operations and covert action can and should be compared in terms of economic operations and paramilitary operations to those of economic and high-end operations that can be seen to have taken place or could take place as part of a cyber offensive operation campaign. From this, therefore, this chapter has clearly established the direct connection between these two types of activities. Further, this chapter has argued that although there are 'new' methods for these types of operations to be used, due to the fact that cyber offensive operations are being used this does not make the activities in fact 'new'. This is because all of these activities can be established to still be economic or paramilitary activity. In addition, as was demonstrated with the part of the chapter that looked at traditional covert action, the fact of the matter is that states have always come up with different types of activity to

target both another state's economy or to conduct a paramilitary operations. From this therefore it is clear that what is being seen with cyber offensive operations is a evolution of covert action rather than something new.

CHAPTER FIVE

Covert Action, Cyber Offensive Operation, and Organisation

This thesis has clearly demonstrated that cyber offensive operations are covert action. Although cyber offensive operations are covert action, this chapter will, nevertheless, argue that, instead of being a form of covert action, as some have argued, cyber offensive operations should be treated as covert action in general rather than merely a form. This is because cyber offensive operations can achieve all of the forms of covert action including paramilitary activities, as it is theoretically possible for cyber offensive operations to conduct assassinations. As such, this author believes that cyber offensive operations should be termed as covert action using cyber means. Further, this chapter will develop the existing theory of covert action. This will be achieved in relation to the ladder of escalation of covert action that has been offered by Johnson and Lowenthal because there is now a need to include covert action that is achieved via cyber means.

Additionally, this chapter will demonstrate that because covert action has been conducted using cyber means, covert action now faces a number of organisational issues that need to be addressed. This argument will be illustrated by looking at the issues that the UK and the US had in the development of the organisation of covert action in the past. It will then demonstrate that states need to learn from past mistakes in creating an effective organisational structure to conduct covert action via cyber means.

Cyber Offensive Operations are not a form of Covert Action

Cyber offensive operations are covert action. Nevertheless, there is a need to establish whether cyber offensive operations are a form of covert action. In 2007, Daugherty stated that a form of covert action was what he termed ‘information warfare’. He stated that information warfare ‘is a fairly new addition to the covert action inventory’.[1] Further, he states that information warfare is ‘either remotely or on-site, a computer, or data banks with the intent of altering or destroying the

[1] Daugherty, ‘The Role of Covert Action’, p. 283.

hardware, software, or information in the computer is considered to be covert action'.[2] Finally, Daugherty states that 'what was twenty years ago was a fledging off-shoot of the intelligence collection is now realizing its enormous potential as a component of covert action'.[3] The reason that the thesis has chosen to build on this was that, although Daugherty has stated that this type of operation has enormous potential, Daugherty only provides fourteen lines on this subject. This thesis thus far has shown that Daugherty was almost correct. Information warfare, or more correctly, cyber offensive operations are happening and they have a direct relationship to covert action.

Yet there are some issues with Daugherty's argument. The research has shown that although cyber offensive operations are covert action, this study would argue that they are not a form of covert action as Daugherty argued. This is because cyber offensive operations are being used for the same types of operations as traditional covert action. If cyber offensive operations were to be considered a form of covert action they would have to be aimed at only achieving one type of activity.

Despite the wide variety of types of cyber offensive operations identified in chapters three and four, they all belong to the types of covert action identified by the covert action theorists, as discussed in chapter two. This is because, as was shown in chapters three and four, the types of operations that cyber offensive operations are used for to conduct propaganda campaigns. Cyber offensive operations were being used for political campaigns. The clearest example of these types of activity have been through the cyber gathering of documents by the Russian state in 2016 and 2017 and targeting the US presidential elections and the French presidential elections.[4] Cyber offensive operations are being used for economic operations; for example, although the main point of the operation does not seem to be directed at achieving this end, the Iranian attack on the Sands casino. The Iranians conducting this campaign caused the company to lose 40 million dollars.[5] Cyber offensive operations are directly connected to paramilitary operations due to the fact that they could be used to conduct assassinations.

[2] Ibid., p. 283.
[3] Ibid., p. 283.
[4] For more information see chapter three
[5] Benjamin Elgin and Michael Riley, 'Now at the Sands Casino: An Iranian Hacker in Every Server' *Bloomberg*, first published on 12.12.2014, http://www.bloomberg.com/news/articles/2014-12-11/iranian-hackers-hit-sheldon-adelsons-sands-casino-in-las-vegas, last accessed on 27.03.2015.

This then leads to the point that instead of seeing cyber offensive operations as a new type of covert action, they are in fact a new method of conducting covert action, rather than a form in the same way that propaganda, political, economic, and paramilitary are each separate forms of covert action. By cyber offensive operations being used for all of these types of operations and being used to achieve the results that were outlined in much greater detail in chapters two, three, and four, it is clear that, cyber offensive operations should instead be described as covert action. They are covert action achieved through cyber means.

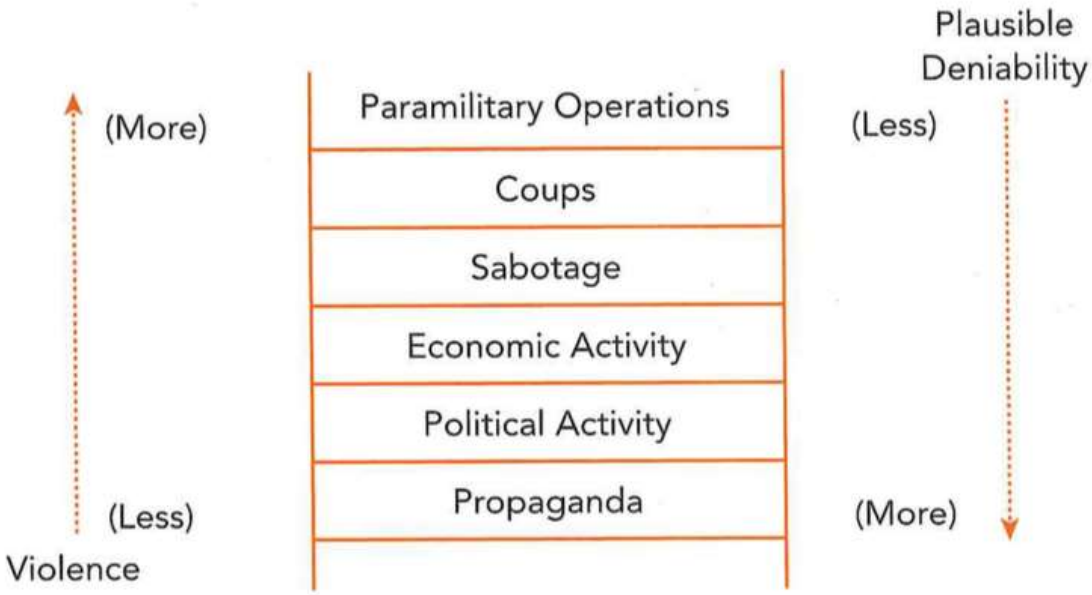
Some authors do treat cyber offensive operations as being covert action rather than a form. This, in this author's opinion is the correct argument to take. In 2017 Lowenthal argued, that cyber offensive operations could achieve propaganda, economic, and sabotage operations.[6] This author has argued that the inclusion of sabotage is flawed. This was demonstrated because the author felt that if a state trained a guerrilla force to destroy another state's power system, these would be termed a paramilitary operation. These operations would also be termed a paramilitary operation if a state used their own intelligence agency to conduct a similar operation. From this, high-end cyber offensive operations should be seen as the cyber means equivalent of paramilitary operations. Further, this thesis has demonstrated in chapters three and four that covert action achieved via cyber means has the potential to achieve more operations than this. From this there is a need to include the new types of covert action. It agrees with the fact that there should be propaganda, political, economic, and paramilitary as the main forms of covert action. Yet, the thesis argued in chapter two that states can and have conduced a type of activity termed direct counter propaganda. In these ways, there is need to reassess the existing understanding of covert action to include this 'new' activity.

This author also takes issue with how Lowenthal assesses the violence with each type of activity. The ladder of escalation that Lowenthal created makes the argument that a sabotage operation would be less violent in terms of action than a paramilitary operation. Yet, as was shown with the Russian covert action initiative against the Ukrainian power plants in 2015-2016, covert action using cyber means can

[6] Lowenthal, *Intelligence*, Seventh Edition, p. 256f.

be used to affect a huge number of people. In addition, as was the case in the 2016 presidential elections, covert action via cyber means can be used to now conduct political operations that go beyond what could reasonably be achieved with traditional methods. Finally, as will be demonstrated below covert action and covert action using cyber means will from time to time need to work in unison to achieve particular operations. In this way, this author believes that although Lowenthal is correct in his argument of not treating cyber as another form of covert action there is still more that needs to be done to clearly demonstrate the types of covert action.

Figure 4: Mark Lowenthal's Covert Action Ladder.[7]



[7] Ibid., p. 257.

Figure 5: New Covert Action Ladder.

In this author's opinion, this is how the covert action ladder should now look. Firstly, this model includes a much more detailed understanding of the different forms of covert action. The violence has been divided up to follow that the least violence is connected to propaganda. However, this is broken down further because social media propaganda has ability to target more people than traditional propaganda and thus should be seen as more violent. The political form of covert action has been split to allow for the level of violence to be seen. The Defacement operations are clearly very low in terms of the violence whereas coups are the highest form of covert action. Economic follows the same pattern as political. Finally, paramilitary has been divided, merging in the high level operations discussed in chapter four, with the traditional paramilitary operations. In this way, both forms of assassination are seen to be the same level of violence. Targeting infrastructure is a higher level of violence than this. In this model, the author argues that affecting critical national infrastructure and the supply and training paramilitary forces are both jointly the most violent form of action. This is because, this author believes that in terms of its level of violence both forms of operations are equal rather than one form being more violent than the other.

Another difference between this ladder and the version of the ladder that was offered by Lowenthal is that, this author's ladder has removed the notion of plausible deniability. There are a number of reasons for this. Firstly, because the original versions of the ladder of escalation, both in terms of the first theory and how it was later adapted to covert action, did not see this as being part of the ladder of escalation.[8] The idea of the plausible deniability as going down in relation to the level of violence, it could be argued is problematic. This is because propaganda is the lowest level of violence, yet the fact that a state cannot be seen to be conducting the operation does not necessarily follow. For example, Radio Free Europe and Radio Liberty were clearly conducting propaganda activities on behalf of the US, so deniability was not achieved. This is equally still clear in the use of other forms of covert action. In paramilitary operations the level of secrecy will depend on what the operation is hoping to achieve. The US in their support of the Mugihadeen against the

[8] The first Ladder of Escalation was from Herman Kahn. Kahn, *On Escalation*, p. 38, The first mention of the covert action forms part of a ladder of escalation appears to be Loch K. Johnson, 'On Drawing a Bright Line for Covert Operations', *American Journal of International Law*, 86:2, (1989), 284-309, this article was reprinted as a chapter in Johnson, *Secret Agencies*, pp. 60-88.

Soviet Union maintained different levels of secrecy throughout the operation. At first they appeared to want to maintain a higher level of secrecy, but once the US started to provide stinger missiles their only real aim in terms of secrecy was to maintain a level of plausible deniability. However, it must be noted that this author is not the first to acknowledge that the nature of secrecy around the use of covert action is fluid. States need at times only to maintain enough secrecy to allow for them to maintain a level of plausible deniability about the operation. This notion is particularly relevant in the use of covert action via cyber means. This can be seen in the fact that the use of political activities in which it can be seen that the level of secrecy changes depending on the activity that is being contemplated. For example, with target and relational activities, the aim of a state in relation to secrecy is merely to maintain a level of secrecy that is enough for plausible deniability. Whereas with the use of resentment activities, it is much more important for a state to maintain a higher level of secrecy. The level of secrecy will also change depending on the activity. For example, when spreading damaging economic information, it is must more important for a state to maintain a higher level of secrecy than it is for a defacement activity. In all of these ways, it is clear that the level of secrecy in both traditional and covert action via cyber means is a fluid concept.

Organisation

The fact that cyber offensive operations are covert action just covert action via cyber means, presents an interesting dilemma for states when using covert action. The biggest dilemma facing states is how to have an effective system to allow for covert action both in its traditional means and cyber means. To understand why this is a problem, it is worth looking at historical examples of where traditional covert action has been placed to see if there are any examples of how this will affect the cyber means of covert action. The second dilemma is the ethics of using cyber means to conduct parts of covert action. This will, however be dealt with in the final chapter of the thesis.

Deciding whether covert action organisations should be placed within either intelligence gathering organisations or the military has a long history. It was argued by Daugherty in 1948 when the CIA was created it was given the role of conducting

covert action over the military because the military wanted no part of it.[9] The British engaged in similar debates. However, this was settled in 1947, by the Minister of Defence who argued that intelligence and covert action should stay within the Foreign Office.[10] In the US, by contrast, the military had on occasion sought to run covert action operations. It is not of course the first time that there have been debates about where covert action should be placed. Traditionally, it was argued by William Daugherty that covert action should not be included within the military and should in fact be in control of intelligence agencies. Abram Shulsky and Gary Schmitt have argued that, according to the US government what is or is not covert action depends on legal definitions.[11] They make reference to the fact that the military could be deployed or develop very similar techniques and operations for the military as are used for covert action. There is clear evidence to support their argument. Take, for example, US operations in Laos and compare them to US operations in Vietnam over the same period. In Laos, the operations were controlled by the CIA and, in Vietnam, they were controlled by the military. Both organisations conducted very similar operations in the sense that both tried to recruit local forces to conduct the fighting.[12] Yet, there was a difference: in Vietnam, the US had publicly declared that they were involved. Whereas in Laos, the US had not publicly declared their involvement.

However, the issue of military involvement with covert action did not end there in the US. In 1995, the Director of Central Intelligence attempted to allow for more covert action organisations within the military.[13] Further, after the attacks of 11 September 2001, then Secretary of Defence, Donald Rumsfeld gave, what to all intents and purposes were covert action operations to the military. For example, in 2004 Special Operations Command were given the powers to 'recruit foreign paramilitary fighters, and purchase equipment or other items from foreigners'.[14] This

[9] Daugherty, *Executive Secrets*, p. 59.
[10] TNA, CAB 301/14, 'Review of Intelligence Organisations 1947 Report by Air Chief Marshal Sir Douglas Evill', Chiefs of Staff Committee, The Secret Service Memorandum by the Minister of Defence C.O.S. (47) 135(0) 30.06.1947, It was also stated in a later review of intelligence that the Foreign Secretary should still be in control of SIS and GCHQ see TNA, CAB 301/17, 'Report of Enquiry by Sir Norman Brook into the Secret Intelligence and Security Services', p. 21.
[11] Abram N. Schmitt and Gary James, *Silent Warfare: Understanding The World of Intelligence* (Washington D.C: University of Nebraska Press, 2002), p. 78.
[12] C.F., for a comparison read John Prados, *Presidents' Secret* Wars, pp. 239-296.
[13] C.F for more information see Ibid., pp. 59-70.
[14] Jennifer D. Kibbe, 'Covert action and the Pentagon', *Intelligence and National Security*, 22:1, 57-74, (2007), 61.

it was pointed out was, historically, the purview of the CIA.[15] Although, under the 1991 Intelligence Authorization Act, covert actions could be conducted by 'any department, agency, or entity of the United States Government' which would include the military, there has, and still is, an on-going legal debate about what this means in relation to the fact that covert action excludes operations that are traditionally military but it is not clear what a traditional military operation actually is.[16] This, then clearly shows that there is a long history in the US of battles over what is covert action and whether the military can conduct these operations.

There are merits to Daugherty's argument about the need to split the two. Firstly, the military works directly for the government.[17] If a soldier or a group of soldiers were used to conduct an operation under international law, these soldiers would have to wear their uniforms to be offered protection under the Geneva Convention. If these soldiers were found to be conducting an activity in another state to say blow up a bridge, this would be an act of war.[18] This would mean that there would be no plausible deniability. The soldiers in their uniforms would clearly be seen to be acting on behalf of the US government.[19] From this, Daughtery's argument about the fact that intelligence agencies should have control of covert action is clearly supported, because of the fact that they will be able to maintain deniability.

For covert action to be successful, as Johnson notes, the covert action people need to understand the intelligence about the country.[20] In this case, it would seem that the most logical place for covert action would then be with the organisation that has this intelligence. Much of intelligence and covert action operations use the same people and technical support. This can be seen in the case of the joint American-British operation to overthrow the Prime Minister of Iran in 1953 in which the main Iranian based agents that conducted the operation were also the same agents that provided the intelligence about Iran.[21] This means that dividing covert action organisations away from intelligence could have meant that an agent would be recruited to work for the same government but for different projects. This would

[15] Ibid., 61
[16] Ibid., 63.
[17] Daugherty, *Executive Secrets*, p. 61.
[18] Ibid., p. 62
[19] Ibid., p. 62.
[20] Johnson, *Secret Agencies*, p. 76.
[21] Aldrich, *The Hidden Hand*, p. 472.

increase the danger to the person who is recruited and the recruiters. Further, covert action presents a clear danger to the function of intelligence, in which, if an operation was conducted it could 'blow' the channels that intelligence organisations have. Finally, intelligence agencies maintain the infrastructure needed for covert action. It was noted by Daugherty, that the CIA maintains the civilian aircraft; they maintain the systems for creating cover stories which are needed not only for intelligence gathering operations, but would also be needed for covert action.[22] From this it has meant that the CIA as a covert action organisation had created the systems that it needed to conduct the both intelligence and covert action. In these ways, it is clear that there is a good reason to see that covert operations should be within an intelligence gathering organisation.

When the US government began to experiment with the organisational structure for the use of cyber offensive operations they faced similar issues of not knowing where the organisation should be placed as they had with covert action.

However, deciding what organisation should maintain cyber means of conducting covert action has become, arguably, even more complicated than traditional covert action. It must be noted that the issue of which organisation should control cyber activities also has a long history. This is because with the addition of the cyber element there are now many organisations that are depended on to allow them to function.

In the US a situation exists in that a military organisation also perform covert action via cyber means.[23] It could be argued that if both of these countries could break down the system and start again, they would and it would probably not be like this. With the recent discussions in the US about the future of US Cyber Command and its relationship to the NSA, it is important to look into the organisational system. By using past experience, it is possible to show that splitting US Cyber Command from the dual hatted nature of the head of the NSA and the head of US Cyber Command presents a number of issues that need to be addressed. By dividing US Cyber Command from the NSA, it appears that they are splitting the parts of the covert action side from intelligence. The reason for this may be that military operations will

[22] Daugherty, *Executive Secrets*, p. 61.
[23] C.F., although the thesis has argument more about the US situation this is because there is less information about the British organisation system than the US. So it may be that the British have an even more confusing situation.

use the same techniques as in covert action, Yet, having multiple agencies working on the same system but for different reasons will inevitably, and already has, cause problems. This argument can be seen in the fact that the Russian attack on the DNC became known because two Russian agencies were trying to penetrate the same system. Russian foreign intelligence had been in the DNC for what appeared to be at least a year, yet, it was not until Russian military intelligence also tried to penetrate the system later, that it became known that someone was in the system who should not have been there.[24] From this, by having two organisations one military and the other one not identified, it caused the operation to be blown.

There are, however, some very good reasons that US Cyber Command should be split from the NSA by the removal of the dual hatted control that the director has over US Cyber Command. Firstly, it was recommended in 2014 by *The NSA Report: Liberty and Security in a Changing World*, that US Cyber Command should be controlled by someone other than the director of the NSA. It was stated that military and intelligence operations are complementary but distinct and should be treated as such.[25] In addition, it was felt that by US Cyber Command and the NSA being controlled by the same person it meant that one person had too much power under their control. Further, having a dedicated Cyber Command would mean that operations would be coordinated more effectively with other US military operations. This would mean that commanders on the ground would have an easier time coordinating cyber operations with their traditional military forces. Another reason that Cyber Command has allegedly been looked into splitting from the NSA is that the NSA is a clandestine organisation. There have been some claims that, because of this, the NSA has stopped US Cyber Command from conducting operations because it wanted to maintain intelligence collection.[26] This has been claimed against operations that Cyber Command have been conducting against IS.[27] Although there have been no confirmed documents that have been publicly presented to support this, it does seem

[24] For more information see chapter three and below.
[25] Richard Clarke, Michael Morell, Geoffrey Stone, Cass Sunstein, and Peter Swire, *The NSA Report: Liberty and Security in a Changing World* (Princeton: Princeton University Press, 2014), p. 137.
[26] Charley Snyder and Michael Sulmeyer, 'Decoding the 2017 NDAA's Provisions on DoD Cyber Operations' *Lawfare*, first published 30.01.2017, https://www.lawfareblog.com/decoding-2017-ndaas-provisions-dod-cyber-operations, last accessed on 10.07.2017.
[27]Lolita C. Baldor, 'US to create independent military cyber command', *The Washington Post*, first published 17.07.2017, https://www.washingtonpost.com/politics/federal_government/us-to-create-independent-military-cyber-command/2017/07/17/ec67a192-6abf-11e7-abbca53480672286_story.html?utm_term=.6636dc29c1a3, last assessed 17.07.2017.

plausible. Finally, the military and intelligence organisations work under different legal authorities. Intelligence operations are controlled by a Title 50 authorisation whereas the military are controlled by Title 10.[28] This would mean that both organisations were clearly shown to be operating under the other control. There seems to be general agreement that overall cyber command and the NSA should be split.[29] It would then seem that it is a question of if, not when, the split will happen. Yet, this means that there needs to be some very robust systems in place to make sure there is still effective coordination and control between the two.

The original policy of US Cyber Command was more in line with the defensive than offensive operations.[30] Yet they have taken a much more active role, and they are now conducting offensive operations. This can be seen in the fact that in 2015 one of its strategic goals was to 'build and maintain viable cyber options and plan to use those options to control conflict escalation and to shape the conflict environment at all stages'.[31] It has become increasingly clear that this also includes conducting covert action using cyber means against foreign adversaries, especially against the Islamic State, as was demonstrated in chapters three and four.[32] From this, by splitting the two organisations it could allow for one to focus more on its original goal.

It is not just the military organisations that have a stake in cyber means of covert action that have caused problems, but there is now a situation where a large number of different intelligence agencies could lay a claim to being the organisation that should run covert action, even the cyber means. In the case of the US, it is four different organisations – the NSA, US Cyber Command, Global Engagement Center,

[28] Clarke, Morell, Stone, Sunstein, and Swire, *The NSA Report*, p. 137
[29] C.F there was general agreement for the splitting of US Cyber Command from the NSA United States Senate Committee on Armed Services, 'Hearing To Receive Testimony On Cyber Policy, Strategy, And Organization' 11.05.2017. In the written statements by all the witnesses Former director of national intelligence, the Admiral James G. Stavridis, USN, Retired, Dean Of The Fletcher School Of Law And Diplomacy At Tufts University And Former Commander, United States European Command and General Michael V. Hayden, USAF, Retired, Principal, The Chertoff Group And Former Director, Central Intelligence Agency.
[30] US Government, Department of Defence, 'Department of Defence Strategy for Operating in Cyberspace', July 2011, p. 5.
[31] US Government, The Department of Defense, 'The Department of Defense Cyber Strategy', April 2015, p. 14.
[32] The National Security Archive, Email from USCYBERCOM to CDRUSACYBER, 'Subj: CYBERCOM FRAGORD 01 to TASKORD 16-0063 To Establish Joint Task Force (JTF)-ARES to Counter the Islamic State of Iraq and the Levant (ISIL) in Cyber Space', Secret//Rel to USA, [Redacted], dated 5.05.2016.

and the CIA – that all have an active role in cyber offensive operations or covert action. In the UK, it would appear to be at least two different organisations: GCHQ and SIS; not to mention the overall planning committees and various other bodies in both countries and those other intelligence agencies that have some stake in cyber. The notion of the CIA and SIS being able to lay some claim to covert action via cyber means is because the CIA and SIS are traditionally the organisations that conduct covert action for the US and the UK. Further, both these organisations, have at least in some level an involvement in cyber operations. The CIA have, clearly, from the evidence that was leaked by *Wikileaks,* looked into developing cyber tools.[33] Although the alleged power of these tools were overblown when they were first reported, the fact that traditional covert action agencies have looked into the cyber tools as a means that they could lay a claim to being the organisation that should run covert action.

SIS state that 'working as part of a cross government effort, SIS provides secret intelligence to help protect the UK from current and future cyber threats from a range of cyber actors whether from hostile states, terrorists and/or criminals'.[34] It was argued by Davies, that due to the fact that the British intelligence system of organisation was based on each organisation being in control of a single source allowed for there to be less friction between the services. That is SIS would collect HUMINT whereas GCHQ would focus on SIGINT and TECHINT.[35] This division of intelligence was created around the nature of the intelligence that was being gathered.

It can also be argued that states such as the US and the UK may find it difficult in attempting to break up covert action into traditional and covert action achieved through cyber means without creating difficulties for both activities. There have been a number of times that states such as the US and the UK have attempted to divide covert action by the methods of conducting it. In the US, in 1948 up until 1952, the Office of Policy Coordination (OPC) functioned as the base for US covert action and was separate from the intelligence collection. OPC was joined with the CIA in 1952 because there was too much competition between the two, which caused problems and was deemed unworkable. It was argued by Rostizke that due to the

[33] For more information see Wikileaks, Vault 7 Files.
[34] SIS, https://www.sis.gov.uk/our-mission.html.
[35] Philip H.J. Davies, 'Intelligence and the Machinery of Government Conceptualizing the Intelligence Community' Public Policy and Administration, 25:1, (2010), 29-46, 39.

official split in the covert action and intelligence in the US from 1948-1952 there was duplication and confusion.[36] Both of these organisations had different liaisons with their customers, both had different procedures for the foreign liaison and both often made contact with the same groups and individuals. When OPC were given control of all forms of covert action each internal group began to see one another as competitors. It was noted by Davies that the political warfare, propaganda warfare, economic warfare, and paramilitary operations saw each other as the competition rather than working together.[37]

It was noted that 'The failure of SO1 (political operations) and SO2 (sabotage) to cooperate in 1940-1, and the experience of PWE itself, has shown that political warfare and subversion should be organised regionally and not functionally'.[38] There are plenty of examples of when organisations have begun with one clear function in which it was found that they were actually are needed to fulfil another function which overlaps. For example, although SOE were only meant to conduct sabotage operations they did engage in political operations. Further, it was argued by SOE's internal historian that

> The main weakness here [in the Balkans] was the lack of any effective coordination between the Balkans countries, between D Section, and other agencies working there, and between the preparations for subversion and those for the conduct of large scale military operations in the area.[39]

This then clearly shows the dangers of splitting covert action by function and having multiple agencies.

Further, covert action and covert action achieved through cyber means can be used in conjunction with each other. This has happened before and it is likely that it will need to happen in the future. To begin with, in the Russian campaign using cyber means during the 2016 US presidential elections there have been some suggestions that Russians may have used agents of influence as part of their campaign against America. It has been alleged that members of President Donald Trump's election team have had contacts with the Russian government in the lead up to the covert

[36] Rositzke, *The CIA's Secret Operations*, p. 150.
[37] Philip Davies, *Intelligence and government in Britain and the United States A Comparative Perspective Volume 1: Evolution of the US Intelligence Community* (Oxford: Praeger Security International, 2012), p. 197.
[38] David Garnett, *The Secret History of PWE: The Political Warfare Executive 1939-1945*, with an introduction by Andrew Roberts (London: St Ermin's Press, 2002), p. xxiii.
[39] William Mackenzie, *The Secret History of SOE The Special Operations Executive 1940-1945* (London: St Ermin's Press, 2000), p. 15.

action campaign. This connection was first seen through the evidence presented in a document created by Christopher Steele who was a former member of SIS. In this document, he alleges that Paul Manafort, Carter Page, Michael Flynn, Michael Cohen all had contact with Russian government officials.[40] In addition to the Christopher Steel document, the fact of some collusion between Trump's team and the Russian government has been a central feature in the hearing of both the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence into Russian involvement in the elections. It has been alleged that both Donald Trump's former National Security Advisor, Michael Flynn, and his Attorney General, Jeff Sessions, had links to the Russian government. Flynn has resigned because of these allegations. However, it must be noted that so far there has been nothing from these committees' hearings which has been publicly confirmed that any of Donald Trump's team were agents for the Russians.

Nevertheless, even this case, there was no collusion or agents of influence, the allegations do demonstrate a way in which states could and, most likely, will bring together traditional covert action and cyber means of covert action. A state will use both to advance their aims, whether it be through using covert action via cyber means to get a person into place and then using this person to influence policy or whether both are used to influence policy. What this shows is that tradition covert action and covert action by cyber means will be used together.

A further way in which covert action via cyber means could be used in connection with traditional covert action is through Online HUMINT Operations (GCHQ term). It was clear from the Snowden leaked documents that, at the very least, GCHQ have looked into the use of Online HUMINT. It is also clear that US cyber Command have also looked into this approach as well.[41] It appears that Online HUMINT operations are operations in which members of an intelligence service make contact with a person and build up a relationship with a person much in the same way as intelligence agents do in traditional HUMINT operations, but they do

[40] Christopher Steele, 'US Presidential Election: Republican Candidate Donald Trump's Activities in Russia and Compromising Relationships with the Kremlin', Company Intelligence Report 2016/080, accessed via https://www.documentcloud.org/documents/3259984-Trump-Intelligence-Allegations.html, last accessed 30.06.2017.

[41] The National Security Archive, Department of Defense, 'Instruction S-3325.10, Subject: Human Intelligence (HUMINT) Activities in Cyberspace', June 6, 2013. Secret/Noforn. http://nsarchive.gwu.edu/dc.html?doc=2692127-Document-19, last accessed on 20.07.2017.

this via cyber means. This could be through forums, through social media, or in some other way via the Internet. The aim appears to be to use these agents for intelligence gathering. Nevertheless, these agents could be used for covert action as well. This could be through using the intelligence agencies to make contacts with non-governmental hacking organisations such as Anonymous or other groups.[42] The intelligence organisations could then use these groups to target particular groups or governments. Although it is merely speculation that this could happen, there is some evidence to show that it is plausible. A document leaked by Edward Snowden, has shown that government intelligence has used what appears to be online HUMINT operations against non-governmental organisations. This was seen in GCHQ targeting Anonymous and the Lizard Squad a private hacking group. Although this operation appears to have been motivated for a criminal investigation, it is not to difficult to imagine that these type of operations could be used to convince these organisations to target groups on intelligence agencies' behalf but without these groups knowing that they are working for a state's intelligence organisation.

Online HUMINT may be used to begin a traditional covert action operation. This is because after a particular intelligence agency has made contact with a particular person or group and cultivated a relationship, the person or group could then be used to conduct traditional covert action. This could be through using the person to spread news stories; it could be through using this person or group to begin political operations; or it could be through using this person or group to begin paramilitary operations. Although there has been no evidence that any of these types of operations have taken place it is not a big leap to think that Online HUMINT operations could be used in this way. This shows that traditional covert action and the cyber means could at times work together in a campaign.

There are, however, two operations that clearly show traditional covert action and covert action via cyber means being used together. The first of these operations took place in 2007 and saw Israel launch a cyber operation against Syria under the codename Operation Orchard. In this operation, Israel used their cyber unit 8200 to target the Syrian air defence network.[43] In this operation, Israel, rather than taking down the Syrian air defence network, changed the system so that the display that

[42] Edward Snowden Document, GCHQ, 'Cyber Offensive Session: Pushing the Boundaries and Action against Hacktivism', ca.2012, Snowden Surveillance Archive.
[43] Rid, *Cyber War Will Not Take Place*, p. 42.

would have shown to the Syrian forces manning the system that planes were approaching instead displayed nothing. This was done through a computer programme called SUTER that disrupts data links between the radar and the computer screen so it would remain blank.[44] The system was not taken off line because, as was noted by Rid, this would have been clear to the Iranians that an operation was taking place.[45] Making the screens of the Syrian air defence network appear as if nothing was there allowed for Israeli warplanes to destroy a nuclear reactor in Syrian. There is some debate about whether this should be seen a military operation where cyber was used as an enabler or whether this should be seen as covert action.[46] However, because this was an unacknowledged use of force, this author believes that this was a covert action operation in which cyber was used in such a way to allow an air strike. This was a little different from how Russia used their cyber forces as an enabler for operations in Georgia in 2008. This is because Russia had not been trying to obscure the fact that their military force was being used in Georgia, whereas the Israelis appear to have tried to achieve the aim of keeping the use of force unacknowledged. This, then, clearly shows that cyber and paramilitary covert action, in the case of Israel, was being used together to conduct operations.

The final event that demonstrates clearly that the cyber means of covert action has been used in conjunction with traditional covert action is Russia's involvement in the Ukraine with operations in the Crimea and Ukraine. It has been argued that the Russians have developed operations in which they will use their power in such a way that it supports proxies and gives itself plausible deniability in its operations.[47] In this, Russia has used, as was shown in chapters three and four, covert action by cyber means through the use of social media, disinformation, political operations, and have even taken down a power station in the Ukraine and the Balkans. The Russians have used cyber means to build up support for their operations. This has included the use of twitter trolls to spread messages, the use of online pro-Russian news organisations. These have all been used to help Russian proxies in the Crimea and it appears to try and spread the actions in the Crimea to surrounding Balkan countries. The Russians have also used paramilitary operations in which proxies who have been supported by

[44] Kaplan, *Dark Territory*, p. 161.
[45] Rid, *Cyber War Will Not Take Place*, p. 42.
[46] Ibid., p. 42.
[47] Oscar Jonsson and Robert Seely, 'Russian Full-Spectrum Conflict: An Appraisal After Ukraine', *The Journal of Slavic Military Studies*, 28:1, (2015), 1-22, 4.

the Russians have been targeting particular areas. The Russians have supplied arms and training to these forces. This has been an important action of the Russians in the Crimea. There has been some theoretical debate about what these types of operations should be termed.

Some see these operations as a form of hybrid warfare or asymmetric warfare in which all powers of a nation are being used to achieve a military objective. However, the Russians have been keen to maintain plausible deniability in these operations. Even when forces have been caught, as has a Russian paratrooper, the Russian government have tried to maintain deniability for these operations. The paratrooper who was caught in the Ukraine was stated to have been there by accident,[48] which would suggest a covert action operation. However, this was changed when Vladimir Putin stated that Russian forces are active in the Ukraine.[49] In this type of operation, it has been shown by the Russians, that it is hard if not impossible to maintain plausible deniability for the operation for a long period of time. This is because the Russian government has used a large military force and their soldiers have maintained poor security. For example, soldiers had uploaded images of themselves in the Ukraine with messages.[50] However, it is likely that other states will use very similar techniques in the future but on a smaller scale. They will use traditional covert action to create, and maintain a paramilitary force and they will use cyber means for conducting covert action to spread a political message and in the case of the power station, to threaten other states. In these ways, covert action will be used together.

From this it is clear that there is now a situation where there is are dangers of different groups all conducting the same operations but working for different ends. This is true of the military's involvement with covert action, dividing the primary intelligence collection agency away from covert action and the fact that different methods of conducting covert action traditional and cyber means. It would then be hoped that in terms of covert action via cyber means states would now be keenly aware that having multiple agencies on closely related tasks is a danger and that they have found a way around this. This is not the first time in which two different

[48] BBC News, 'Captured Russian troops 'in Ukraine by accident'' *BBC* News, first published 26.08.2014, http://www.bbc.co.uk/news/world-europe-28934213, last accessed 10.07.2017.
[49] Jonsson and Seely, 'Russian Full-Spectrum Conflict' 4.
[50] Ibid., 4.

intelligence organisations have relied on the same methods. During the Second World War, MI5 and SIS worked together to coordinate the work of controlling and maintaining the agents that the Germans thought were working for them but were in fact working for the British. To achieve this, the Twenty Committee was created.[51] This committee coordinated the work of the double agents and the information that was given back to the Germans. Davies has demonstrated other times in which different intelligence organisations have worked together.[52] It is hoped that a similar situation could be created to allow for the effective coordination of these operations.

There is the appearance of some levels of higher control of operations, in which different agencies and outside personnel can discuss the use of covert action and authorise plans for their involvement. In the US, you have the National Security Council and the UK, also, as of 2010, the National Security Council. This seems to allow for different organisations to bring forward plans for covert action. In this way, it means that covert action can be coordinated at a higher level.[53] This can, if it is based on some other previous organisations who have had a similar role, for example, the Official Committee of Communism Overseas, have the ability to look into long-term operations and bring together various organisations.[54] Nevertheless, it seems to be difficult for this to be of great effect on day-to-day issues. It would be of much more use for agencies to have a lower level committee, which, instead of having senior members discussing the use of operations, you bring together people from the organisations at the mid level who work on the operations together. It may be difficult for such a system to work. It would also create a separate operation together in which agencies would have to bring together plans. However, it would be the mid-level people who would have the clear understanding of what they will be doing in terms of the operations; it will also allow for people to compare the operations that each organisation is conducting and deal with issues in the internal planning stage. This notion is not without historical precedent and it can lead to effective collaboration between parts of different organisations, even if the organisations themselves may, in fact, be in conflict. Although it is well documented that SOE had a troubled

[51] For more on this committee see J.C. Masterman, *The Double-Cross System The Incredible True Story of how Nazi Spies Were Turned into Double Agents* (Guilford: Lyons Press, 2012).
[52] Davies, 'Intelligence and the Machinery of Government', 29-46.
[53] Rory Cormac, Michael S Goodman, and Tom Holman, 'A Modern Day Requirement for Co-Ordinated Covert Action', *The RUSI Journal*, 161:2, (2016), 14-21, 14.
[54] Lomas, *Intelligence, Security and the Attlee Governments*, p. 130.

relationship with SIS,[55] parts of these two organisations were able to work effectively together at different times. There are many examples when the mid-level of these organisations had managed to work together effectively. In France and Belgium both organisations, due to the fact that they were divided into a country system, were able to maintained liaison with each other.[56]

The use of this mid-level connection is also supported by Johnson. Johnson argued that covert action operations should include people from outside the covert action side and those who have expertise on the country or organisation that is being attacked.[57] There should be an extended and not only covert action specialist, whether they are on traditional or cyber side, but also those with the outside knowledge to discuss the plans. This may increase the likelihood of the success of the operation. Further, this system would allow for both covert action organisations to coordinate the plans at an early stage.

It is not just internal structures that need to be addressed in relation to covert action achieved through cyber means, but also international systems as well. States have, and likely will, continue to have increased coordination internationally between themselves in relation to covert action. The coordination between states in covert action is nothing new. The US and the British have worked together on joint operations from the Second World War, during the Cold War, and clearly, they have at the very least coordinated cyber tools and techniques that both sides have created to help each other. Nevertheless, it is clear that issues have arisen in the relationships when both states and organisations have different priorities when it comes to covert action. Take for example British attempts to remove the Iranian Prime Minister. This had begun a lot longer than those of the US. Also, even when both organisations were working together in the operation there were still, at times, problems in the relationship. It was noted that although for the most part both organisations worked together well, with SIS officers, apparently aiming to make every effort to get along with the CIA, it was noted that there were tensions in the SIS-CIA relationship in the

[55] Robert Cecil ‘‘C’'s war’, *Intelligence and National Security*, 1:2, 170-188, 177; MRD Foot J.M. Langley *MI9: The British Secret Service that fostered Escape and Evasion 1939-1945 and its American counterpart*. (London: The Bodley Head, 1979), p. 42; Jeffery, *MI6*, p. 354.
[56] William Mackenzie *The Secret History of SOE* P.382
[57] Johnson, *Secret Agencies*, p. 83.

Nicosia station (a station is the main operating place within a country).[58] It is interesting to note that in the lessons learned section of the internal history it was made clear that 'the lesson here is clear. As in the larger world picture, US-UK interests and activities must be coordinated. A great deal is to be gained by direct coordination in special fields of activity once both parties have recognized that their aims are really identical'.[59] From this, it is clear that states have been able to work together in relation to traditional covert action activities.

It could be argued that international coordination faces an even greater need to be coordinated between states than traditional covert action. This is because; the internet by its very nature is multinational. If different states have different priorities, it can mean that confusion could be created through the use of these activities. If different states are looking to conduct a political campaign against a particular state, it could mean that if they do not coordinate and both operations become ineffective. Covert action via cyber means tools that target variability have direct dangers for many different countries.[60] This is not that the weapons themselves could target them, but, because once vulnerability has been targeted, states and private organisations will look to patch these vulnerabilities. This will mean that there will need to be coordination between the states' organisations that use these types of operations who could likely have an issue whereby one state targets a vulnerability then other states that have developed these tools to target these vulnerabilities will become obsolete. Although, this will only apply to some of the covert action by cyber means, it is still an important area in which states should look to cooperate or at least make sure that they only target vulnerabilities that would have been of more effective use against a more important adversary.

It is likely that the coordination will include not only the US and the UK but also the other 'Five Eyes' partners (see Introduction). However, this presents further issues in the need for coordination. In addition, as was noted, there is clear historical

[58] The National Security Archive, Dr. Donald Wilber, CIA Clandestine Service History, "Overthrow of Premier Mossadeq of Iran, November 1952-August 1953," March 1954, by. Chapter X, What was Learned from the operation, p. 87, http://nsarchive.gwu.edu/NSAEBB/NSAEBB28/10-Orig.pdf last accessed on 25.04.2017.
[59] Ibid., p. 87.
[60] Jeppe T. Jacobsen, 'The US and Europe Need to Coordinate Their Cyber Weapons', *Defense One*, first published 26.04.2017, http://www.defenseone.com/technology/2017/04/us-and-europe-need-coordinate-their-cyber-weapons/137346/?oref=d-channeltop, last accessed on 27.04.2017.

evidence that this has already happened. For the most part, it seems that states have been able to coordinate covert action, and there does not seem to be any real evidence that indicates that this would not be as effective in terms of covert action by cyber means. Moreover, in the case of the 'Five Eyes' and covert action by cyber means, it may be that they will actually be more successful in terms of international coordination than they have before. This is because the groups that are taking the lead have had agreements to coordinate intelligence from the Second World War onwards. However, what is missing is what internal discussions organisations have about the coordination. Nevertheless, it is unlikely that in the case of the Five Eyes international coordination will cause a great deal of issues. In this way, with the use of covert action but through the use of cyber means, it is clear that states like the Five Eyes will work together to coordinate their operations.

However, it must be noted that there is some evidence to suggest that it has been possible to run successful operations with multiple agencies working together and even working with other intelligence agencies outside of the country of origin. Although there is still very little information about how this worked, it is hoped that there were some lessons to learn from these operations that have been taken forward and even improved. It has been argued that the operation that is commonly referred to, as Stuxnet was an operation that combined the NSA, the CIA and the Israeli SIGINT and Cyber operations group called Unit 8200. In this operation, the NSA found out that the system that was needed to be targeted and the code that was needed along with the Unit 8200 and the CIA could be used to plant the virus because the system was air capped and so had no internet connection.[61] What this does show is that it is possible that multiple agencies can work together in terms of covert action conducted using cyber means. However, it is still possible that a much more effective system could be found that would possibly help to stop the issue of having multiple different countries agencies working together on one operation. This would help stop any repetition of some of the issues of control of traditional covert action that have happened in the past.

[61] Kaplan, *Dark Territories*, pp. 205-211.

Conclusion

It is clear that cyber offensive operations are covert action – just covert action achieved through cyber means. The fact that these activities are aimed at changing behaviour, are an unacknowledged use of force, and that they fall below the threshold of war, means they are covert action. However, these activities are not merely another form of covert action. They achieve all types of covert action that was identified in chapter two. This means that the traditional ideas of covert action had to be challenged and adapted. In these ways, this author created a new covert action ladder that allowed for a more detailed understanding of covert action and covert action achieved through cyber means.

Nevertheless, it is equally clear that the nature of traditional covert action and covert action achieved through cyber means creates a situation in which there is a need to create effective organisational systems to deal with these mounting issues and is something that needs to be thought through by Governments. Using historical examples, it is clear that there are a number of potential issues that might come about from the use of covert action by cyber means where there is a need for coordination. It is clear that having many different organisations, some conducting intelligence, some conducting military operations, some conducting some types of operations, means that there is a real danger of having too many different groups who will fail to work together. There are plenty of examples where the CIA did not get on with its covert action half when it was created in 1948 up until 1952. Overall, it would be hoped that a system might be in place in both Britain and America that has already been worked out but which is secret and has not been made public. If not that, the people working inside the various agencies have, themselves, to come up with various systems so that the lessons of historical examples are not lost. However, this chapter highlighted some of these issues so that others could be made aware of them in the hopes that history will not repeat itself.

CHAPTER SIX

Ethics and Covert Action

Having established in the previous chapter that cyber offensive operations should be seen as covert actions – but covert action achieved through cyber means – it is important to understand whether states could attempt to use these types of activities ethically. In 2017, Lowenthal addressed, both in terms of traditional covert action and covert action using cyber means, the ethics of these types of activities.[1] However, Lowenthal's work did not include any clear answers as to whether or not ethics could be applied, beyond the fact that 'for most citizens, the trade-off between ethics and increased security is accepted, provided that the intelligence community operates with rules, oversight, and accountability'.[2] This, in this author's opinion, does not establish the ethics of covert action or covert action achieved through cyber means sufficiently. This chapter will establish the ethics of covert action and covert action using cyber means.

The reason that the ethics of covert action can be addressed is that, as Toni Erskine argued, the organisations and the agents that work within these organisations can be seen to be 'moral agents'.[3] This is because they can be deemed to make decisions and that, as such, they can also be deemed to have assessed the actions and the consequences of those actions.[4]

There are sources that have addressed the ethics of cyber offensive operations. However, these are in relation to cyber offensive operations and war. For example, in 2017 George Lucas published *Ethics and Cyber Warfare*.[5] Even though this author and Lucas are addressing most of the same actions, Lucas' argument focuses on war and warfare. Yet, as was argued in chapter five, the ways that these activities are being used are covert action, just covert action using cyber means. This, then, requires the author to understand whether the ethical implications of these operations need to be readdressed.

---

[1] Lowenthal, *Intelligence* Seventh Edition, pp. 444-460.
[2] Ibid., p. 460.
[3] Toni Erskine, "As Rays of Light to the Human Soul'? Moral Agents and Intelligence Gathering', *Intelligence and National Security*, 19:2, (2004), 359-381, 362.
[4] Ibid., 362-363.
[5] George Lucas, *Ethics and Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare*, (Oxford: Oxford University Press, 2017).

In this way, this chapter will address the ethics of covert action and then demonstrate that there are minor differences between the ethics of covert action and covert action achieved through cyber mean in terms of the risks of covert action achieved through cyber means facing additional complications due to their use, most notably that they have unintended consequences.

The ethical framework that will be used in this chapter is that offered by Just War Theory (JWT), in which there are six *jus ad bellum* principles that affect the understanding how far an action is ethical. These are: just cause, just intentions, reasonable chance of success, proper authority, last resort, and proportionality. It will also address the issue of civilian immunity that can be seen to be the corner stone of *jus in bello*. Finally, this chapter will assess the use of the ladder of escalation and its relationship to war, covert action, and offensive cyber effects operations and how it affects the understanding of ethics.

The author has chosen to use JWT to assess the ethical issues of covert action, as this has been the dominant means through which the ethics of intelligence and covert action is addressed.[6] One of the first scholars to address this subject was Michael Quinlan.[7] In addition, there have been a number of authors who have looked into what ethical considerations affect covert action. This includes with the work of Loch Johnson and the collection of essays in Jan Goldman's series *Ethics of Spying: A Reader for the Intelligence professional*.[8]

Some take issue with the use of JWT in relationship to intelligence because, with war there is an expectation of a limited use, whereas intelligence can be, and should be conducted almost constantly. Intelligence is conducted constantly because

[6] Angela Gendron, 'Just War, Just Intelligence: An Ethical Framework for Foreign Espionage', *International Journal of Intelligence and CounterIntelligence*, 18:3, (2005), 398-434; Michael Quinlan, 'Just intelligence: Prolegomena to an Ethical Theory', *Intelligence and National Security*, 22:1, (2007), 1-13; David Omand, *Securing the State*, (New York: Columbia University Press, 2010), pp. 261-287; David Omand further highlights JWT in relation to intelligence in Sir David Omand and Mark Phythian, 'Ethics and Intelligence: A Debate', *International Journal of Intelligence and CounterIntelligence*, 26:1, (2013), 38-63, Omand references, 46-55, 58-61; Ross W. Bellaby, *Ethics of Intelligence: A New Framework*, (London: Routledge, 2014), pp. 25-38; Ross W. Bellaby, 'Justifying Cyber-intelligence?', *Journal of Military Ethics*, 15:4, (2016), 299-319. Others included partial reference to JWT in relation to intelligence Michael Herman, 'Modern Intelligence Services: Have They a Place in Ethical Foreign Policy', in Harold Shukman (ed) *Agents for Change: Intelligence Services in the 21st Century*, (London: St Ermin's Press, 2000), p. 307f.

[7] Quinlan, 'Just intelligence', 1-13.

[8] Johnson, *Secret Agencies*; Jan Goldman (ed), *Ethics of Spying: A Reader for the Intelligence Professional* (Lanham: Scarecrow Press, 2006); and Jan Goldman (ed) *Ethics of Spying: A Reader for the Intelligence Professional Volume 2* (Lanham: Scarecrow Press, 2010).

this is how intelligence functions.[9] In addition to this, others, such as Lowenthal, who, although he made references to those who used JWT, stated that in relation to the Just War criteria, 'in the abstract this is a compelling list … But policy makers do not act in the abstract'.[10] This implies that for Lowenthal, JWT does not work as ethical criteria in relation to the covert action.

Lowenthal is not alone in his criticism of the use of JWT. It has been argued by Dipert, that JWT cannot be used in relation to cyber tools because they are so different from traditional warfare. Dipert demonstrated this because cyber tools can be used for many different operations. He points out that cyber tools can be used for intelligence gathering, actual damage, and, then, as assessment of the damage.[11] This thesis has shown this to be, at best, a problematic argument and, at worst, incorrect. Dipert's argument misses the point that the same methods can have different uses. A human agent can gather intelligence, conduct a sabotage operation, and assess what damage their operation actually caused. From this, each action should be treated differently. However, even those that are critical of JWT, such as Mark Phythian stated that 'the work done in this area has represented one of the most thoughtful dimensions of Intelligence Studies in recent years'.[12]

There have been those who have looked into the applicability of JWT to cyber operations but the focus has usually focused on the cyber war or cyber warfare,[13] for example, James Cook. Although, this author feels that Cook has mischaracterised the use of cyber offensive operations, he does, however, argue that 'JWT concerns itself primarily with effects rather than means or media'.[14] Effects can be judged by what the activities are being used for. It is clear, therefore that there is a need to assess the effect of JWT on covert action using cyber means.

[9] Mark Phythian in Omand and Phythian, 'Ethics and Intelligence: A Debate', 43.
[10] Lowenthal, *Intelligence* Seventh Edition, p. 460.
[11] Randall R. Dipert, 'The Ethics of Cyberwarfare', *Journal of Military Ethics*, 9:4, (2010), 384-410.
[12] Mark Phythian in Omand and Phythian, 'Ethics and Intelligence: A Debate', 42.
[13] Mathew Beard, 'Just War, Cyberwar, and Cyber Espionage' in Jai Galliott and Warren Reed (eds) *Ethics and the Future of Spying: Technology, National Security, and intelligence collection* (London: Routledge, 2016); John Arquilla 'Ethics and Information Warfare', in Z. Khalizad, J. White and A. Marshall (Eds), *Strategic Appraisal: The Changing Role of Information in Warfare*, (Santa Monica, CA: RAND Corporation, 2000); Colonel James Cook, ''Cyberation' and Just War Doctrine: A Response to Randall Dipert', *Journal of Military Ethics*, 9:4, (2010), 411-423; Christopher J. Eberle, 'Just War And Cyberwar', *Journal of Military Ethics*, 12:1, (2013), 54-67.
[14] Cook, ''Cyberation' and Just War Doctrine', 416.

The importance, of JWT is that, although it is a cultural construct, the fact is that many of the legal norms of international law are based on JWT; it is a logical ethical framework to use.[15] Further, it has been argued that JWT 'so assigns (moral) meaning to war, and establishes our relation to it'.[16] It was also argued that JWT allows a researcher to deal with issues that would normally be seen as wrong but in certain circumstances, should be allowed.[17] JWT creates the basis for an ethical theory of war that guides the person to understand how a war can be ethically launched and how it can be ethically prosecuted. This allows for a new discipline that considered the application of JWT in relation to intelligence. In these ways, it is clear that, although there are issues with JWT as an ethical framework, it offers the best framework to use.

The Importance of Ethics

It was argued that ethics and morality have a different status to law. They have influence and authority even if governments have not ratified them.[18] It was argued that the reason that is it so important to understand the ethics of these types of activities, it is argued, is that intelligence organisations are not constrained by the same types of legal rules.[19] This is supported by Gendron who argued that, 'ultimately, informal influences and mechanisms must be relied upon to counter any tendency by intelligence agencies to circumvent formal controls and abuse their power'.[20] Andregg argued that even though, at times, states may ignore ethics in the same way they may ignore laws, humans are better for having them in place.[21] From this, it is clear that even if a government chooses not to believe in ethics, they are still applied to their actions.

Understanding the ethics of these operations is also important because it has been argued that it helps those who authorise an operation to understand if the actions

[15] Lucas, *Ethics and Cyber Warfare*, p. 44.
[16] Cian O'Driscoll, 'Learning the Language of Just War Theory: The Value of Engagement', *Journal of Military Ethics*, 6:2, (2007), 107-116, 109.
[17] Ross W. Bellaby, 'Justifying Cyber-intelligence?', *Journal of Military Ethics*, 15:4, (2016), 299-319.
[18] David L. Perry, *Partly Cloudy: Ethics in War, Espionage, Covert action, and Interrogation*, (Plymouth: Scarecrow, 2009), p. 3.
[19] Lucas, *Ethics and Cyber Warfare*, p. 34.
[20] Gendron, 'Just War, Just Intelligence', 401.
[21] Michael Andregg, 'Ethics and Professional Intelligence', in Loch K. Johnson (ed), *The Oxford Handbook of National Security Intelligence*, (Oxford: Oxford University Press, 2010), p. 742.

should be undertaken. Johnson argued that ethics allows policymakers to judge what should be allowed and under what circumstances.[22] William Colby (former director of the Central Intelligence Agency) argued that ethical and moral considerations help to understand which actions should be allowed.[23] Further, Johnson argued that 'those in the intelligence business (intelligence officers), as well as those responsible for guiding them (policy officials in the executive branch and lawmakers on Capitol Hill), may ignore ethics – but only at great peril to the nation's reputation, not to mention their own'.[24] The argument is that, if a state acts unethically in their activities, it can have domestic political effects as well as international effects. Further, simply arguing that a country acted legally is not enough to establish that a country has acted ethically.

A further reason that ethics in intelligence is important is that it has been shown that the use of immoral actions via a state, in both general foreign policy and intelligence gathering, can cause an intelligence agency difficulties in being able to recruit agents. Taylor and Snow illustrated that the Soviet Union was less capable of being able to recruit agents. This was because the Soviet Union found it difficult to recruit agents using ideology as a recruitment tool after the horrors of Stalinism and the repression in Hungary became known.[25] Although this was not presented as an argument for ethics, it does show that being seen to be, in some way, 'good' could benefit states in the recruitment of agents and being 'bad' may deter those who might have worked for that state if it had a better reputation for being moral.

In addition, there have been a number of studies which have argued that, by the US and their allies being presumed to have conducted or to have been in any way involved in torture, their ability to gather intelligence was affected. It was noted by the Senate investigation into enhanced interrogation (which many in the media and non-governmental organisations such as Amnesty International describe as torture) that the US damaged intelligence sharing relationships.[26] This then shows that by

[22] Johnson, *Secret Agencies*, pp. 69-72.
[23] William E. Colby, 'Public Policy, Secret Action' *Ethics and International Affairs* 3:1, 61-71, 62.
[24] Loch K. Johnson, 'Ethical Intelligence: A Contradiction in Terms?', in 'A Symposium on Intelligence Ethics', *Intelligence and National Security*, 24:3, (2009), 366-386, 367.
[25] Stan A. Taylor and Daniel Snow, 'Cold War Spies: Why They Spied and How They Got Caught', *Intelligence and National Security*, 12:2, (1997), 101-125.
[26] Senate Select Committee on Intelligence 'Study of the Central Intelligence Agency's Detention and Interrogation Program' approved December 13, 2012 Updated for Release April 3, 2014 Declassification Revisions December 3, 2014 Executive Summary, p. 16.

being seen to be unethical affected the ability of the US to gather intelligence by limiting intelligence relationships.

The practice of gathering intelligence either through HUMINT or through methods such as torture are not the only practices that raise moral questions, all intelligence operations face the same issues. Mass surveillance, for example, which, it should be pointed out is not a new area of intelligence professionals' work. During the Church Committee's investigations into the actions of intelligence organisations, they found that the US were conducting mass surveillance of their own populations.[27] This led to questions on the ethics of such operations. The questioning of these practices has become a further issue recently with the Edward Snowden files that caused questions about whether what they were doing was justified.[28] This led to many groups questioning what the 'Five Eyes' intelligence community were actually doing and what spy agencies should do.

The final reason that it is important that intelligence agencies act ethically is that, as Omand argued, 'the golden rule of intelligence is whatever is claimed by one side in the way of intelligence methods should be expected of the others to also claim'.[29] From this, it can be supposed that if states such as US or Britain conducted a covert action activity unethically, it is more likely that another state would conduct activities in the same manner to benefit from the argument 'well you did it too'. In these ways, it is clear that the ethics of covert action is an important area that needs to be addressed.

Just War Theory and Covert Action

The first ethical principle related to JWT is just cause. Just cause in war, it has been argued, is usually related to self-defence or the defence of others. Within the United Nations Charter, Chapter VII it was argued that a just cause would be created out of the actions of others in that, if a state invaded or used an armed attack against another

[27] United States, Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, 'Final Report Of The Select Committee To Study Governmental Operations With Respect To Intelligence Activities United States Senate Together With Additional, Supplemental, And Separate Views Intelligence Activities And The Rights Of Americans Book II', see for example p. 343f.
[28] After the leaking of information from Edward Snowden issues relating to bulk collection were changed with the passing of USA Freedom Act.
[29] Omand, in Omand and Phythian, 'Ethics and Intelligence: A Debate', 53.

state, the state that was attacked, or a number of states, can respond to this using the justification of self-defence.[30] From this, the just cause is created out of the right to self-defence. It has also been argued that the defence of others using the self-defence of the UN Charter is a feature of just cause.[31]

The other just cause that is related to self-defence principle has been termed the culpability of the victim.[32] In the case of a country being invaded, the argument would be that the person who has invaded removed their immunity to not be attacked. Finally, the culpability of the victim has been likened to the just cause for war in humanitarian interventions. Tesón argued that, by denying human rights, a government would lose their right not to be invaded for the purpose of humanitarian intervention.[33] With this then, if the political system that is in place inside a county is denying the rights of its people a just cause can be created.[34]

The just cause principle in relation self-defence clearly presents a difficult situation in how it is applied to covert action. This is because the state that conducted the activity may appear to the aggressor rather than an agent within the just cause of self-defence. This can be explained by using an example from chapter two, Operation HOUSEPARTY. In Operation HOUSEPARTY, the plan was to create a fear inside the Soviet Union of their intelligence services by planting information that 'showed' their own agents were working for the British. This would not follow the idea of a clear principle of self-defence in that the British could be argued to have been the ones to have been the instigators of the aggression as they were planting the fake information about the Soviet Officials.

Nevertheless, within just intelligence, it is generally accepted that just cause for gathering intelligence is created out of the fact that a nation has a right to self-defence from threats to national security.[35] Yet, even here, there is a difficulty in understanding what actions are classed as self-defence or national security. During the

[30] UN Charter, Chapter VII, Article 38, and Article 51, http://www.un.org/en/sections/un-charter/chapter-vii/ the part on the security council will be covered below under the proper authority principle.
[31] George P. Fletcher and Jens David Ohlin, *Defending Humanity: When Force is Justified and Why*, (Oxford: Oxford University Press, 2008), p. 146.
[32] Mathew Beard, 'Just War, Cyberwar, and Cyber Espionage', p. 107
[33] Fernando R. Tesón, 'Eight Principles for Humanitarian Intervention', *Journal of Military Ethics*, 5:2, (2006), 93-113, 96.
[34] Michael Walzer, *Just and Unjust War A Moral Argument with Historical illustrations*, Fifth Edition, (Philadelphia: Basic Books, 2015), p. 53.
[35] Ross W. Bellaby, *Ethics of Intelligence*, p. 27.

Cold War, economic interests were not usually counted as national security threats; however the economy has begun to be linked with national security, in which case economic interest could be allowed for a self-defence argument to be used.[36] Although there have been debates about which dangers a state faces are reasonable for them to make a claim of self-defence, it has been argued that a just cause related to self-defence can only exist if the threat that a state is facing is high enough to justify the actions. This argument of national security being a just cause in relation to just intelligence is supported by Gendron who argued that just cause is created out of the need for self-defence, but states that the claim self-defence 'must be real and not spurious'.[37] From this, as long as the dangers are real, even if there were economic dangers, then a state would be able to claim that they were in fact acting in self-defence.

The just cause for covert action should usually be based on the idea that actions are dealing with a national security threat or helping the citizens of the state who are conducting the operation.[38] This has been referred to as self-defence.[39] From this, the argument would be that Operation HOUSEPARTY was linked to the right to the defence of national security; then the covert action activity would be justified. The self-defence must be based on the idea that the threat is real and is not spurious. With this it can be seen that the just cause has also been linked with the whether the action is based on significant need.[40] But as with the case of just intelligence, it must be a real threat to national security.

The self-defence just cause principle in relation to covert action has, in the same way as war, been linked to the defence of others. Take for example, the operations to help democratic parties in Europe in the late 1940s, early 1950s, these operations were used to help those parties resist the actions of what was viewed as non-democratic parties. It was argued that there was evidence, although it was not made public, that the Russians were providing funds to the leader of the Italian Communists.[41] It was argued by William Colby, the former director of the CIA, that

[36] See for an example of economics being linked with national security see HM Government 'Intelligence Service Act 1994' Section 1 2(B) and Section 3 2(B).
[37] Gendron, 'Just War, Just Intelligence', 418.
[38] Charles R. Beitz, 'Covert Intervention as a moral problem', in Jan Goldman (ed), *The Ethics of Spying A Reader for Intelligence Professionals*, (Maryland: Scarecrow Press, 2006), p. 209.
[39] Colby, 'Public Policy, Secret Action', 63.
[40] Beitz, 'Covert Intervention as a Moral Problem', p. 211.
[41] Perry, *Party Cloudy*, p. 167.

the campaign in Italy allowed democratic forces to obtain their own goals.[42] It was argued that without the support of the covert action campaign, the communists would have won the election.[43] From this, it can be seen that the just cause was created out of the fact that the covert action was in response to the action of others, thus a defence of others is a clear ethical principle for covert action.

The second principle of JWT is the question of whether the actions that a state wishes to take have just or right intentions. Darrell Cole states that intention is based on what the war aims to achieve.[44] A just cause of the war could be to defeat aggression. Whereas, just intention is what you plan to do in the war. From this, Cole argued that the intentions principle is not only based on what a state plans to do in an operation but it is also based on whether or not the acts were consistent with the stated intentions.[45] In this sense, it means that a state could not argue that a war has a just cause if their intentions in the war change and show that their cause was not what was publicly stated. Take for example a humanitarian intervention; if a state declared that that they were going to intervene because a leader of another state was killing his own people but the actions of the state that went to war based on the killing then took economic advantages of this country, this would show the actions to be unethical. This then clearly demonstrates the difference between cause and intentions. Iain Atack argued, that this demonstrates the importance of the just intention criteria. This is because it allows for an assessment of the just cause to test that it is not just being used as a way to justify actions.[46] In this way, the actions that a state wishes to take must be related to the just cause of the activity to be deemed ethical.

In relation to covert action, it has been argued that deciding what creates the just intentions is centred on the notion of a number of tests: the objective of the country that conducted the activity, whether the covert action that targeted a foreign power works, what the results will be to the country, and whether the covert action benefits the international community.[47] It has also been argued that the just intentions

[42] William E. Colby, with Peter Forbath, *Honorable Men: My Life in the CIA*, (New York: Simon & Schuster, 1978), p. 115.
[43] Gallo, 'Covert Action', 355.
[44] Darrell Cole, 'War and Intention', *Journal of Military Ethics*, 10:3, (2011), 174-191 175.
[45] Ibid., 188.
[46] Iain Atack, *The Ethics of Peace and War: From State Security to World Community*, (Edinburgh: Edinburgh University Press, 2005), p. 65.
[47] James Barry, 'Managing Covert Political Action', in Jan Goldman (ed), *Ethics of Spying: A Reader for the Intelligence Professional* (Lanham: Scarecrow Press, 2006), p. 260.

in covert action are to repel or to help address a wrong depending on what changes a state wishes to be done.[48] However, there have been a number of operations that have, at least partially been linked to economic reasons. In the case of Guatemala, one of the reasons that the US had been looking to targeting them for a covert action campaign was because American companies could have lost out to a land reform deal.[49] With the fact that economic security has now been linked to national security, an economic argument for a covert action could be seen as a grey area. However, using the same argument as just cause the intention should be real and not spurious.[50] From this, it can be seen that the just intentions is a key principle is assessing the ethics for covert action programs.

A further principle of JWT is whether or not the actions that are being taken have a reasonable chance of success. The principle states that war should not be undertaken if there is little to no chance that a level of success that is measurable will be met.[51] It has been argued that the criteria for this principle is that the chance of being successful is reasonable, not certain, but better than a hope of success.[52] In addition, it has been argued that the reasonable chance of success can be seen as not just a military victory but also a political victory.[53] This was supported by Fotion who argued that stopping the enemy from having a complete victory may meet the definition of success.[54] Overall, then, it can be seen that in relation to traditional JWT, the principle must be that there is a higher than likely chance of success but what is meant by success will depend on the activity.

In terms of intelligence, it has been argued that the principle of reasonable chance of success still applies.[55] Omand also argued that the reasonable chance of success criteria should include an assessment of the unintended consequences of the use of these operations, such as political fallout from the operation.[56] This seems to be

[48] Ibid., p. 260.
[49] David L. Perry, '"Repugnant Philosophy": Ethics, Espionage, and Covert Action', in Jan Goldman (ed), *Ethics of Spying: A reader for the Intelligence Professional*, (Lanham: Scarecrow Press, 2006), p. 235.
[50] Gendron, 'Just War, Just Intelligence', 418.
[51] Nicholas Fotion, *War and Ethics: A New Just War Theory*, (London: Continuum International Publishing Group, 2007), p. 19.
[52] Frances V. Harbour, 'Reasonable Probability Of Success As A Moral Criterion In The Western Just War Tradition', *Journal of Military Ethics*, 10:3, (2011), 230-241, 232.
[53] Ibid., 232.
[54] Fotion, *War and Ethics: A New Just War Theory*, p. 114.
[55] Omand, *Securing the State*, p. 287.
[56] Ibid., p. 287.

the same type of questions that covert action programs should answer to decide if the operations should be conducted. There should be a clear understanding of what success in a programme would look like. In addition, success should be seen as not just a hope of success, but a reasonable chance that this would be achieved.

James Barry argued that, in relation to covert action, the test of whether this principle is achieved should be that if there are any dissenting opinions on the likelihood of success, these should be looked at carefully.[57] In addition Stempel argued the likelihood of success should also be assessed in relation whether or not an activity becomes known. This is because if an activity becomes known, whether a success or not, it can affect the reputation or cause blowback which affects further foreign policy objectives.[58] An example of this in the Iran contra affair in which, when the US were supplying arms to Iran, it caused large political issues with a long-term ally of the US – Jordan. This is because it was noted that Jordan were refused weapons systems that the US were supplying to Iran even though the US had campaigned for a complete arms embargo of Iran.[59] The Iran-Contra affair was where members of the US government would sell arms to Iran and then use the money that they made to secretly supply the Contra who were opposed to the government of Nicaragua.[60] This means that even if a covert action is successful there can be consequences. Using these questions as a starting point, a state must make sure that they address the likelihood of the success of a covert action activity based on the dangers of this activity becoming public.

Another test of the reasonable chance of success are the unintended consequences of the operation.[61] This could be that covert action could work in the short term but that, in the long term, states could face problems.[62] This can be seen in Anglo-US coup against Iran in 1953. After, the US and the UK conducted the successful covert action campaign to remove Mohammad Mosaddegh in 1953, they replaced him with the Shah of Iran who repressed his own people and was clearly seen as an American puppet. Because of the actions of the Shah, it has been argued

[57] Barry, 'Managing Covert Political Action', p. 261.
[58] John D. Stempel, 'Covert Action and Diplomacy', *International Journal of Intelligence and CounterIntelligence*, 20:1, (2007), 122-135, 129.
[59] Daugherty, *Executive* Secrets, p. 57.
[60] Stempel, 'Covert Action and Diplomacy', 129.
[61] Loch K. Johnson, *Secret Agencies*, p. 76.
[62] Loch K. Johnson, *Secret Agencies*, p. 76.

that this created much resentment towards the US and the West and more generally.[63] From this, the short-term successes of the covert action could be argued to be outweighed by the long-term failure of resentment towards the West. In this way, states should understand the reasonable chance of success criteria and the implications of what success actually means.

The next principle of JWT, is that the person who decides to conduct the war must have proper authority to do that. Traditionally, the proper authority has been held by the leader of a country or the parliament of a country.[64] This had been seen as an important criteria because it stops warlords or private citizens from bringing a country into a war rather than the commander of the state. Walzer argued that proper authority rests on the notion that the authority has the consent of the nation.[65] Although to some extent the proper authority could now be argued for a war would not an individual state but it would rather be that of an international organisation like the United Nations. This is because, the states that are signatories to the UN charter have agreed that the Security Council is the right level to determine when a war is in effect and the actions that can be used.[66] However, there are debates as to what extent proper authority for war should rest with international organisations. For example, Fotion notes that international organisations now compete with states on the authority for war but does not make clear if one has a stronger claim than the other.[67] Brown argued that although multinational organisations do have some claim to the proper authority criteria, overall proper authority should still rest with states themselves, rather than international organisations.[68] In this way, it can be seen that there has been some debate as to who has the proper authority to agree to a war, a state's leader or the multinational organisation the UN.

The proper authority principle is very important area in how ethics of covert action are assessed. The idea is that covert action programs should only be launched if the person who has proper authority to make this decision on behalf of the state agrees to it. This is so the agents of the organisations that conduct covert action themselves

[63] Andreas Etges, 'All that Glitters is Not Gold: The 1953 Coup against Mohammed Mossadegh in Iran', Intelligence and National Security, 26:4, (2011), 495-508, 505f.
[64] Fotion, *War and Ethics*, p. 18
[65] Walzer, *Just and Unjust War*, pp. 61-63.
[66] See UN Charter, Chapter VII, http://www.un.org/en/sections/un-charter/chapter-vii/.
[67] Fotion, *War and Peace*, p. 115.
[68] Davis Brown, 'Judging The Judges: Evaluating Challenges To Proper Authority In Just War Theory', *Journal of Military Ethics*, 10:3, (2011), 133-147, 139.

do not launch the activities on their own operations. This has, traditionally, been one of the claims levelled against the CIA.[69] In the case of the US, this would be the president; in the UK ,this would be the prime minister or a minister of state. However, in the US, the proper authority has, to some extent, been extended to include other bodies as well as the president.[70] Although, oversight is not usually included as a basis for proving proper authority has been achieved, it was argued by Omand that proper authority is helped and strengthened by having oversight.[71] He stated that 'external oversight can then provide added reassurance or corrective pressure if problems emerge'. [72]

In the US, the oversight role has been achieved through the creation of two committees that provide oversight of intelligence agencies and for covert action the President must inform the circle of eight leaders of the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence of the operation, either straight away, or in extraordinary circumstances, within a timely fashion.[73] This has been interpreted as 48 hours.[74] In this way, the House and the Senate would be able to say whether the operation should be allowed to continue. In terms of covert action, it has been argued that it, in fact, faces greater oversight than any other activity that the CIA actually conduct.[75]

In addition to these organisations being able to be seen by oversight committees, the US Senate Armed Service Committee and the Senate Select Committee on Intelligence can cut off funds for operations. Further, the House Permanent Select Committee on Intelligence has control in different ways for aspects of the US intelligence community budget.[76] It was argued by Ott that the power to cut off funds for US covert action programs has been used in the past, although he does

[69] William C. Prillaman and Michael P. Dempsey, 'Mything the Point: What's Wrong with the Conventional Wisdom about the C.I.A', *Intelligence and National Security*, 19:1, (2004), 1-28, 7-10.
[70] Barry, 'Managing Covert Political Action', p. 252.
[71] Omand, in Omand and Phythian, 'Ethics and Intelligence: A Debate', 54.
[72] Ibid., 54.
[73] US Government, 'Intelligence Authorization Act, Fiscal Year 1991', Section 503, Paragraph 5, C 1 and 5 and C 3.
[74] Marvin C. Ott, 'Partisanship and the Decline of Intelligence Oversight', *International Journal of Intelligence and CounterIntelligence*, 16:1, (2003), 69-94, 79.
[75] Daugherty, *Executive* Secrets, pp. 29-31.
[76] Gregory C. McCarthy, 'GOP Oversight of Intelligence in the Clinton Era', *International Journal of Intelligence and CounterIntelligence*, 15:1, (2002), 26-51. For details on the control of the Senate Select Committee on Intelligence and Senate Armed Services Committee see 29, for the House Permanent Select Committee on Intelligence see 39.

not provide details as to which programme this was used for.[77] From this it was argued that, it gave Congress, in their oversight role, an almost veto over covert action programs.[78] In this way, in the case of the US, the proper authority principle for covert action has been extended to the oversight committees.

In the case of the UK, the oversight of intelligence agencies, is performed by the Intelligence and Security Committee (ISC). It was argued by Phythian that this committee has had, at best, only achieved a mixed success rate in providing oversight.[79] Peter Gill argued that although there have been some cases where the ISC exceeded expectations, it focuses too much on the management of intelligence agencies rather than providing oversight.[80] Part of the problem was originally caused by the mandate of the ISC. The mandate was designed to examine expenditure, administration and policy of MI5, SIS, and GCHQ.[81] The mandate of this committee was extended with the passing of the Justice and Security Act 2013 which allowed it, at times, to consider operational matters around the intelligence agencies.[82] However, there are still flaws in the ISC oversight role. For example, in 2016 when the ISC conducted an inquiry into the use of a drone to kill Reyaad Khan (see chapter 2), the Prime Minister was able to refuse to hand over information to the committee.[83] From this, it shows that, although the British have attempted to establish an oversight system, they have not been as successful as the US. Nevertheless, overall, the fact that there is an oversight system in the UK does in some ways mean that proper authority has been strengthened by the ISC.

The principle of proper authority in the case of covert action does, however, have issues. It has been argued that using the military to conduct covert action, allows for much looser oversight than intelligence agencies traditionally face when they were conducting covert action programs.[84] In the case of the US, the use of the military for such operations has meant that, although the covert action can include any branch of

[77] Ott, 'Partisanship and the Decline of Intelligence Oversight', 78f.
[78] William J. Daugherty, 'Approval and Review of Covert Action Programs Since Reagan', *International Journal of Intelligence and CounterIntelligence*, 17:1, (2004), 62-80, 64.
[79] Mark Phythian, '"A Very British Institution": The Intelligence and Security Committee and Intelligence Accountability in the United Kingdom', p. 702.
[80] Peter Gill, 'Evaluating Intelligence Oversight Committees: The UK Intelligence and Security Committee and the 'war on terror'', *Intelligence and National Security*, 22:1, (2007), 14-37, 32.
[81] Gill, 'Evaluating Intelligence Oversight Committees', 21.
[82] HM Government, 'Justice and Security Act 2013, Chapter 18' Part 1, Section 2(1).
[83] HM Government, Intelligence and Security Committee of Parliament, 'UK Lethal Drone Strikes in Syria', published 26.04.2017, Paragraph 9, p. 2f.
[84] Jennifer D. Kibbe, 'The Rise of the Shadow Warriors', *Foreign Affairs*, 83:2, (2004) 103.

the US government, traditional military operations have been exempt. What this has meant in practice has been that in some cases, most notably the use of drones for assassinations, they fall outside of traditional oversight areas of both the House and Senate intelligence committees.[85] It has been pointed out that even if there is a joint operation in which intelligence agencies and military personnel are working together on the same operation, they could operate under different authorities. This, then, presents issues to the level of oversight that the people face. For example, the military does not have to submit to Congress in times of war information about an on-going operation. This has been compounded by the fact that the military does not have to tell Congress about anticipated hostilities where US forces are involved. [86] Nevertheless, operations will still be reviewed at different times and this shows that proper authority can still be achieved even if it is less in the case of the military than it is for intelligence agencies.

In relation to cyber warfare, Lucas stated there was no real difference in the just cause, just intention, or proper authority principles.[87] However, not everyone agrees with this interpretation. In terms of research into the ethics of cyber offensive operations, the argument is that cyber offensive operations face the same just cause criteria as just war, even if there may be problems in understanding how a state may be able to 'prove' that another state has conducted the operation. The argument is that just cause is created out of the self-defence requirement and an act of war.[88] Yet, the issue with this is that these authors still follow the notion that cyber offensive operations are cyber war, rather than looking at the operations as covert action achieved using cyber means.

The author believes that in terms of just cause, just intention, and proper authority there are only two slight differences between covert action and covert action achieved through cyber means. Firstly, states may view cyber as offering less chance of getting caught than with traditional covert action and may try to use these activities for causes which fall below the level of just cause. John Arquilla also argued that, with what he referred to as cyber war states 'may feed temptation to skirt classical guidelines about going to war justly, I think it is quite possible that cyber-strategy and

[85] Ibid., 107.
[86] Ibid., 103.
[87] Lucas, *Ethics and Cyber* Warfare, p. 103.
[88] Edward T. Barrett, 'Warfare in a New Domain: The Ethics Of Military Cyber-Operations', *Journal of Military Ethics*, 12:1, (2013), 4-17 7, Eberle, 'Just War And Cyberwar', 55-57.

tactics may make waging war justly a bit easier'. [89] This is because if states feel that the actions will not become known they may think that they would not need to explain or justify their actions to the same level affecting the just cause and just intention principles. Secondly, in terms of proper authority, the actions should still be sought in relation to activities, as they would with traditional covert action. It has been argued that states could hide the use of these tools and remain invisible from proper authority.[90] Yet covert action has a clear basis for the activities. The fact is that cyber means of covert action would, in the case within inclusion of oversight actually have higher proper authority than even that of war. The issue still is that these operations do have, in the case of the US, as was highlighted in chapter five, a question of whether these activities fall under intelligence agencies or the military. This is compounded by the fact, as was shown in chapter five, that both organisations are controlled by the same person under the dual hatted nature of their role. Although this has been argued to change at some point, so far, this has not happened. This, then, has meant that the issue of proper authority has been difficulty to achieve to the same extend as with covert action.

In terms of the principle of reasonable chance of success, there are two issues with the use of cyber means for conducting covert action that states should be aware of. Firstly, it could be argued that with covert action achieved through cyber means, there is an issue of something akin to a Pandora's box effect.[91] This is related to what Omand referred to as unintended consequences.[92] This issue can be seen in the Stuxnet operation. Singer argued that due to the fact that the Stuxnet operation had the unintended consequence of other states conducting similar operations. This was because if one state has already conducted the operations, others may conduct similar operations.[93] From this it is clear that, as Omand argued, 'whatever is claimed by one side in the way of intelligence methods should be expected of the others to also claim'.[94] If states do believe that others have used a covert action using cyber means unethically then it may cause the affect that other states will use this as justification of

[89] John Arquilla, 'Twenty Years of Cyberwar', *Journal of Military Ethics*, 12:1, (2013) 80-87, 84.
[90] Cook, 'Cyberation' and Just War Doctrine', 418f.
[91] P. W. Singer, 'Stuxnet and its Hidden Lessons on the Ethics of Cyber Weapons', *Case Westren Reserve of International Law*, 47:3, (2015), 79-86, 86.
[92] Johnson, *Secret Agencies*, p. 76.
[93] Singer, 'Stuxnet and its Hidden Lessons on the Ethics of Cyber Weapons' 86.
[94] Omand, in Omand and Phythian, 'Ethics and Intelligence: A Debate', 53.

their own operations. Therefore this, indicates that states should assess the unintended consequences of the activities in relation to the Pandora's box effect.

However, there is an argument that some of these activities are not particularly new and thus all covert action even with the inclusion of covert action achieved through cyber means, it could be argued, face this issue. Nevertheless, with some of the highest levels and the ability to actually kill someone using cyber, this will become a real issue. The dangers of it must not be overblown but must be kept in mind. This is clearly an ethical question that GCHQ took on board. It was argued in a document that was leaked by Edward Snowden about the guidelines for submission of information to the Secretary of State, that officers should try to understand if this operation or the tools they were using was novel.[95] This suggested that, at least in the British experience with the ethics of covert action via cyber means, states have looked into the unintended consequences of the Pandora's box effect. Finally, this author believes the issue of the Pandora's Box will diminish over time as more states use these types of activities. From this, the fact of a 'new' type of operation will diminish.

One final issue with the principle of reasonable chance of success is that even if a state is successful in conducting an operation there is a chance that there will be the unintended consequence. It can be argued that with the use of cyber means of conducting covert action there is a danger that the tool that was used may spread beyond the original country that was targeted. In case of Stuxnet, the malware appears to have spread well beyond its intended target in Iran as it infected many other countries as well.[96] In this case, it is possible that the malware could have affected systems the tool was not supported to affect (although it appears to have been programmed not to do so). From this, it can be argued that states need to understand the issues of reasonable chance of success and the unintended consequences of the tool spreading. In these ways, states that use covert action via cyber means should address, or at least consider the same questions of reasonable chance of success as with covert action, but make sure they understand that cyber means do face further questions in relation to unintended consequences.

[95] Edward Snowden Document, GCHQ, 'What's the Worst That Could Happen?' edwardsnowden.com, p. 1.
[96] Falliere, Murchu, and Chien, 'W32.Stuxnet Dossier Version 1.4', p. 5.

The next principle of JWT is that the actions need to be of last resort. It is argued that war should only be conducted as a final option.[97] However, the last resort principle is not simply based on the notion that diplomacy has failed and, therefore war is ethical. This is because diplomatic discussions can continue for a long time and there is always a claim that diplomacy could still have worked.[98] Bellamy argued that 'last resort demands that actors carefully evaluate all different strategies that might bring about the desired ends, and selecting force if it appears to be the only feasible strategy for securing those ends'.[99] The criteria of last resort is related not to trying less violent options first, but that a state has consciously considered these options first and can show why these would not work. Further, it can be argued that last resort can be deemed to exist when a state is in imminent danger. This argued was demonstrated in Walzer who examined the Caroline case of 1842. It was argued that the British had been justified in their actions of attacking those citizens who had were planning to attack their ship the Caroline in 1842 because there were no other option than to attack.[100] This has however, always presented issues in understanding what the last resort should be. States can look on other states with suspicions, and as Walzer points out, these can, after the fact, be shown to be incorrect.[101] This means that a state and ethicist are forced to assess at what level something should be seen as having reached the level of last resort. However, overall it could be argued that each case must be judged on its own as there can never be any set standard in which a theory could cover all the issues of whether the principle of last resort has been reached. On the issue of certainty, it has been argued that the level of certainty for the last resort would have to be around 90 per cent sure that the target nation would attack.[102] This shows that, although the actions should be linked, firstly, to trying to achieve a diplomatic situation, it is not always necessary to have tried diplomacy first for an action to be counted in a last resort ethical dimension.

In terms of intelligence, it has been argued that last resort as a principle does not work due to the fact that espionage rather than other means of gathering

[97] Christoph Bluth, 'The British Resort to Force in the Falklands/Malvinas Conflict 1982: International Law and Just War Theory', *Journal of Peace Research*, 24:1, 1987, 5-20, 14.
[98] Helen Frome, *The Ethics of War and Peace: An Introduction*, (London: Routledge, 2011), p. 62
[99] Alex J. Bellamy, *Just Wars: From Cicero to Iraq*, (Cambridge: Polity Press, 2006), p. 123.
[100] Walzer, *Just and Unjust War*, p. 74.
[101] Ibid., p. 79.
[102] Randall R. Dipert, 'Preventive War and the Epistemological Dimension of the Morality of War', *Journal of Military Ethics*, 5:1, (2006), 32-54, 48.

intelligence is usually the only way.[103] However, as was argued above, a state does not need to try the less violent means first. They need a reasonable belief that the less violent option would not work. This argument is supported by Bellaby and Omand who both argued they do not need necessarily to have to try other means, they just have to have a strong belief that the other means would not work.[104] Further, Gendron's '"last resort" must be interpreted not as a process which first exhausts the contributions of open and less intrusive sources, but as one which matches the objective, the time frame, and the permeability of the target to the means used'.[105] In this way, the principle of the last resort is that states have to have a reasonable belief that their actions are the only actions that would work.

This, then, should be the joint criteria for a last resort principle for covert action, diplomacy should be tried if possible but if it would not work the covert action agency must demonstrate a reasonable belief as to why it would not work. This is similar to Barry who argued that they should have tried or at least be able to show why other less violent means would not work before covert action is used.[106] In addition, it has been argued by Patterson and Casale, using a similar framework of last resort, that targeted killing could be deemed ethical if there was no other way.[107]

However, the principle of last resort does have issues in relation to covert action. In terms of intelligence gathering, it is argued that the last resort is achieved through the fact that if the intelligence could be gathered by open source means then these should be used rather than the covert intelligence gathering.[108] Yet, with covert action the level of last resort is based in part on what a country 'might' do rather than what a country 'will' do. From this, the last resort principle faces an issue. The fact that a country might do something leads to the question about whether this is enough to argue that last resort has been met. This is that the actions can be based on the idea that something could happen but it has to be something reasonable that a person could base that assessment on. It could be argued that the last resort principle should be

[103] Phythian, in Omand and Phythian, 'Ethics and Intelligence: A Debate', 43.
[104] Bellaby, *The Ethics of Intelligence*, p. 28, and, David Omand in Omand and Phythian, 'Ethics and Intelligence: A Debate', 54.
[105] Gendron, 'Just War, Just Intelligence', 418.
[106] Barry, 'Managing Covert Political Action', p. 260.
[107] Eric Patterson and Teresa Casale, 'Targeting Terror: The Ethical and Practical Implications of Targeted Killing', *International Journal of Intelligence and CounterIntelligence*, 18:4, (2005), 638-652, 646f.
[108] Bellaby, *Ethics of Intelligence*, p. 28.

linked with the notion of real and not spurious concerns, as was the case of just cause, and using the notion of around 90 per cent certain will help to achieve this. From this it would set a fair ethical notion of last resort.

The last resort principle faces no more greater difficulty in its applicability towards covert action achieved through cyber means than it does in relation to tradition covert action. However, not every one agrees with this statement. It was argued by John Arquilla that 'last resort also comes under pressure when the virtual domain is added into the conflict mix. Cyberwar is a means that can be used early, easily, and highly effectively'.[109] However, this author would argue that this is not the case. The problem with Arguilla's argument is that it was still based on the notion of cyber war, rather than covert action. The principle of last resort should be followed. The state that is conducting the operations should clearly be able to demonstrate that they have either tried to use other means such as diplomacy first, or that it would not work. It could be argued that the main danger is that states will become too keen on using covert action via cyber means because of the feeling that they will not become known and not establish the last resort principle. Further, as Barry argued, states should have to justify, even within the use of last resort, why they would use a more aggressive option than other forms of the same activity.

Another principle of JWT is that the actions that are used must be proportional to the threat that is faced. It has also been pointed out that the proportionality must be linked to everything that is bad and only some things that are good. Bellaby has argued that good can only be calculated to the just aims of the war and incidental benefits do not count towards the good. However, all the 'bads' are counted against the goods.[110] This requirement, it has been argued, could mean that the actions that are taken, for example killing, are overridden by the good that is being achieved.[111] This clearly fits into the argument about the issues of covert action in the sense that the reasons for the actions to be taken must be better than the damage caused. However, in the same way Bellaby argues that actions should not just be related to actual physical harm but all harm that may be caused.

[109] Arquilla, 'Twenty Years of Cyberwar', 84.
[110] Bellaby, *The Ethics of Intelligence*, p. 35.
[111] Jeff McMahan, 'Just Cause for War' *Ethics and International Affairs*, 19:3, (2005), 1-21, 3.

In terms of covert action, it can be argued that the same criteria must met for the action to be deemed to be proportional. This is that states should only choose the option that meets the threat that is posed. In addition, states should consider all the ways that covert action can produce harm and not just focus on physical harm. This is similar to Beitz' who argued that states should have to face additional questions if the use of manipulation is to be justified.[112] From this, the argument is that although paramilitary operations, may be the only form of traditional covert action that produces physical harm, states should address the fact that propaganda can manipulate others, and, therefore, this too produces harm. This argument about the targeting of civilians via covert action also increases with the level of violence of the campaign. The use of economic operations which, even though they are aimed at the state, have the ability to harm the civilian population as you are affecting the stability of another country's economy causing a loss in borrowing power of that state so that civilian services may be affected. An economic operation may also stop the sale of domestic machinery and goods. This will cause a direct loss to the civilian population. In these ways, all forms of covert action produce harm and should be assessed in relation to the threat they are trying to meet.

There are no particular 'new' issues raised by the use of covert action achieved through cyber means as compared to covert action. For example, using cyber propaganda still targets civilians in same way as covert action. However, it has been argued by GCHQ that in terms of propaganda, cyber operations have greater appeal and are more effective than the traditional propaganda.[113] This would mean that using them, intelligence agencies should, in terms of JWT, face a higher proportionality threshold due to the fact these are more 'violent'. Even with higher operations, there is no real difference in the proportionality to that of covert action. In addition, as was noted above, there is a danger that the level of threat in which they are being used may be lower than their traditional counterpart as states may believe that they will not be discovered. However, to some extent, this has already been shown to be a false premise as there are a number of cases that have become public knowledge.

[112] Bietz, 'Covert Intervention as a Moral Problem', p. 213.
[113] Edward Snowden Document, GCHQ, 'Full Spectrum Cyber Effects SIGINT Development as an Enabler for GCHQ's "Effects" Mission', ca.2010, p. 4, Snowden Surveillance Archive.

A further principle of JWT, but one focused on *jus in bello*, is that in a war, civilians have immunity from being targeted. This has also been termed distinction.[114] This principle has been related to proportionality.[115] However, in war, it is generally accepted that civilians should be off limits from the fighting. Every soldier understands that they should not target civilians, even if they do not always follow it, and that, when they do, there is a good reason for this. However, even in war, the civil immunity is a contentious issue. The issues around this principle have been demonstrated by several authors. For example, it has been argued by Walzer that in an extreme emergency, civilians lose their immunity due to the proportional nature of the threat.[116] Further, Deakin demonstrated the issue of Special Forces being discovered by a shepherd and whether the Special Forces soldiers should be allowed to kill the shepherd if they believe that the shepherd may give away the position of the soldiers.[117] From this, it is clear therefore, that, even in war, there is an argument that the principle of civilian immunity is not absolute.

This presents a number of problems when looking at covert action. In covert action, depending on what the operation is looking to achieve, they may directly target civilians. Propaganda, for example, is clearly directed towards civilians. Propaganda and the targeting of civilians with propaganda does not produce the same amount of harm, clearly, as aiming a gun at a person's head. From this, the argument is directly related to the issue of 'harm'.[118] To assess the issue of 'harm' it was argued that states should consider using the legal premise of proximate cause in which you follow a test of a reasonable perception of likely injury.[119] This then would allow states to assess the likely injury from the actions. There is, however, a danger of unintended consequences of the activity. If it is successful in changing a group of behaviour then a state may target those who are dissenting with repressive actions. This is equally applicable to targeting those who are near to terrorist organisations. If an organisation feels threatened, it can look to aggressively suppress those who they may feel are working against them and then supress them in aggressive manners. This

[114] Asa Kasher, 'The Principle of Distinction', *Journal of Military Ethics*, 6:2, (2007), 152-167
[115] Gary D. Brown, 'Proportionality and Just War', *Journal of Military Ethics*, 2:3, (2003), 171-185, 174
[116] Michael Walzer, *Just and Unjust Wars*, p. 267
[117] Stephen Deakin, 'Wise Men And Shepherds: A Case For Taking Non-Lethal Action Against Civilians Who Discover Hiding Soldiers', *Journal of Military Ethics*, 10:2, (2011), 110-119, 110-111
[118] Bellaby, *The Ethics of Intelligence*, p. 35.
[119] Colby, 'Public Policy, Secret Action', 63.

has increasingly been the case with IS who, it has been reported, conducted aggressive repression of people under their territorial control. This can be linked to the threat that the IS felt other propaganda holds towards the population. Using the lowest level of 'violent', it clearly indicates that, for actions to be seen as ethical, states must assess the level of harm in all their uses of covert action achieved through cyber means. Further, it needs to consider that harm is achieved in a number of different ways. All of this shows that the use of propaganda does have implications in who it targets even though we may see it as something close to benign.

In these ways, it is clear that the six principles of JWT can be applied to covert action. States, before they use covert action, should critically assess the use of covert action to these six principles and clearly understand what implications of the operations. In relation to cyber means of conducting covert action, it is clear that there are some issues with how these are applied. Most notably, the issue of unintended consequences in the fact that there may be, with some of the activities, an issue of a Pandora's Box effect, and the fact that some operation, as was the case of Stuxnet, may spread beyond the country that was the intended target.

Ladder of Escalation

With JWT, although there are six individual principles, each of these principles relates to the one another. The only real principle that is apart from the others is the issue of proper authority. Just cause affects the issue of last resort; proportionality to the threat is related to the issue of just cause. Just intentions has a bearing on how the just cause is accessed. To help understand how these issues are interrelated it has been argued that there is a need to use the ladder of escalation. Herman Kahn developed the ladder of escalation in relation to escalation in international crises. This relates to how a state should respond to a crisis and the threshold for that response.[120] Although Kahn did not explicitly relate the ladder ethics in general or to JWT, it has been argued that a ladder of escalation allows the researcher to understand both the level of harm, proportionality, and the just cause.[121] In addition, Johnson used the ladder of escalation when he assessed the ethics of both intelligence and covert action. Using the ladder that this author created (see chapter five) allows the ethics of covert action

[120] Kahn, *On Escalation*, pp. 38-41.
[121] Bellaby, *Ethics of Intelligence*, p. 30f.

and covert action achieved through cyber means to be assessed using the JWT principles. It was argued by Bellaby that, by using the ladder, it becomes clear that the more violent or aggressive a type of operation is, the higher the level of justification using the JWT principles would need to be.[122] Using this as the basis, it is clear that different types of covert action would need higher levels of justification depending on the level of violence of the operation. From this, a covert action campaign that is using the type of activity called 'traditional propaganda' would need the lowest level of justification. In relation to covert action, it can be seen that, although Colby did not term it as the ladder of escalation, he argued that it is less intrusive to use covert action than it is to launch a military invasion.[123] Therefore, it can be seen that where less violent means are being used earlier, there is a lower just cause. From this, the argument is that it is more ethical to target a country earlier via the use of less violent actions rather than wait and use more violence later on. From this, not only is the ladder of escalation an important tool to understand the issues surrounding the level of violence of an activity, it also allows for both intelligence professionals, government officials, academics, and the general public to understand and conceptualise the principles of JWT in relation to types of covert action.

The ladder of escalation that the author created in the fifth chapter is perfectly suited to discussions on the use of covert action and covert action achieved through cyber means. Because of the fact that types of activities follow the level of violence, it means that states and ethicists can use this to address the ethics of each activity. In these ways, using the ladder of escalation makes it possible to assess the ethics of covert action in both its traditional methods and cyber means.

Other Ethical Issues

Beyond the explicit JWT principles, others have come up with other ethical issues that states should address in relation to covert action and intelligence. The most notable of these is Johnson in *Secret Agencies* who came up with eleven ethical guidelines.[124] Many of these have already been addressed within this chapter. The idea of diplomacy first (last resort), being in line with public policy (just cause and

[122] Ibid., p. 30f.
[123] Colby, 'Public Policy, Secret Action', 65.
[124] Johnson, *Secret Agencies*, pp. 60-88.

just intentions); understanding outside issues and not focusing on only using covert action operatives when deciding if an operation should go ahead (proper authority and reasonable chance of success); never violate US laws; avoid targeting democracies as these have more legitimacy unless they have done something which violates their legitimacy; use the idea of less aggressive options first (last resort, proportionality, and the ladder of escalation); making sure the foreign agents know that they will be terminated as an asset if they violate laws which are seen as highly important, like not conducting terrorism and human rights abuses; considering the international reputation of the state that is conducting the operation.[125]

However, there are two further ethical guidelines that need to be looked at. First is whether the actions can be justified to the general public if they became known; this would help to argue that the actions are ethical. However, there are issues with this as a guideline because it would allow states to conduct operations that would otherwise be seen as unethical. Take, for example, torture. In 2014, a poll was conducted in the US in which 59 per cent of respondents stated that torture should be allowed.[126] Even in a more recent poll, conducted after the release of the Senate Select Committee on Intelligence into the use of extreme interrogation (what some have termed torture), 46 per cent agreed, 30 per cent opposed, 24 undecided. Using the guidelines that Johnson offered, this would mean that the action of torture would be allowed. This then would be why, it could be argued, allowing something to be deemed to be ethical because it can be explained to the general public should not be included as an ethical argument. In addition, it was argued by David Perry that what is ethical is not about what people find to be ethical.[127] From this, the author would argue that just because an action can be explained to the general public and they agree with it, this should not be enough to claim that something is, in fact, ethical.

The final guideline that Johnson offered is the idea that 'in almost all cases, policymakers, should reject secret wars, coups d'état, and other extreme measures, for if American interests are so jeopardized, as to require major intervention, then

[125] Ibid., p. 83f.
[126] Adam Goldman and Peyton Craighill, 'New poll finds majority of Americans think torture was justified after 9/11attacks', *The Washington Post*, first published 16.12.2014, https://www.washingtonpost.com/world/national-security/new-poll-finds-majority-of-americans-believe-torture-justified-after-911-attacks/2014/12/16/f6ee1208-847c-11e4-9534-f79a23c40e6c_story.html?utm_term=.5b5462b69329, last accessed 06.02.2017.
[127] Perry, *Partly Cloudy*, p. 3.

properly authorized overt warfare – ideally multinational … is more appropriate and honourable'.[128] However, this author believes that this is flawed. Take for example, the covert action to supply military equipment to the mujahedeen in the 1970s and 80s. If the US had sent in US military personnel to Afghanistan, there could have been a risk of an open war between the two powers. From this, this author would argue that it would seem flawed to suggest that it would have been more ethical to invade Afghanistan in the 1970s and 80s rather than supply arms. This argument can also be seen to apply to a cyber equivalent: the Stuxnet operation. At the time, there were discussions about what would happen if Iran had acquired a nuclear weapon. It is possible that this may have included a military operation. From this, it would seem unclear as to why it would be more ethical for forces to invade Iran and possibly risk another situation like the wars in Iraq and Afghanistan than using these covert action methods. Finally, political operations can have the same effects as those of secret wars; propaganda can lead to the same deaths if they are conducted well. Although, in general, the author agrees with most of Johnson's guidelines, the two that are of question are the justification to the public, although overall this is a good option but has issues. Whereas, the notion of removing the most aggressive forms of covert actions would simply mean that states would have to use more violence means simply because they are overt.

Conclusion

By understanding that cyber offensive operations are covert action just achieved through cyber means, this chapter addressed the ethical implications of these activities. It found that the use of covert action using cyber means does not face any different ethical considerations than covert action. Using a JWT approach, it is clear that, although there are ethical issues to covert action using cyber means, these relate to, for the most part, covert action in general rather than covert action achieved through cyber means in particular. This chapter has demonstrated that there are six ethical principles of JWT related to covert action: just cause, just intention, proper authority, last resort, reasonable chance of success, discrimination, and, proportionality. It has also illustrated the ways that these should be applied to covert

[128] Johnson, *Secret Agencies,* p. 84.

action achieved through cyber means. In addition, this chapter has also argued that a state should also use the ladder of escalation to further help them to understand the ethics of covert action and covert action achieved via cyber means. To do this, the author argued that using the ladder that was created in chapter five of this study allows for ethics of covert action and covert action achieved by cyber means to be effectively assessed.

Further, this chapter has argued it is clear that there is a strong basis for states to use these types of activities ethically. This is because, being seen to be ethical can allow states to recruit and maintain agents. In addition, although this chapter argued that there were some new ethical dimensions to the use of covert action by cyber means, these will likely diminish over time as more states use these forms of operations in the future. The other areas of ethical questions that have been identified by others around the use of cyber offensive operations can clearly be explained by looking at JWT or how JWT is applied to Intelligence.

This then shows that it is clearly important that academics and governments begin to see cyber offensive operations as covert action being achieved through cyber means. This is because so much of what states do is based on having clear definitions of the actual events and what they are being used for.

Conclusion

The purpose of this thesis was to understand if a relationship exists between covert action and cyber offensive operations. There was a need to undertake this research because although in 2007 Daugherty argued that a relationship existed between these two activities, there was not much information on this point.[1] At the time of writing this thesis, there was beginning to be an acceptance that covert action and cyber offensive operations are interrelated. In 2014 Brantly expanded upon the relationship, although he only focused on two examples of cyber offensive operation and how they are related to covert action.[2] In 2017, Lowenthal developed the argument about the relationship between the activities further.[3] Nevertheless, Lowenthal's work still only contained a limited amount of research on the relationship between cyber offensive operations and covert action.[4] This thesis has illustrated the connections between covert action and cyber offensive operations more clearly.

This study has uncovered and demonstrated that, although there is a clear relationship between cyber offensive operations and covert action, it is an imperfect relationship within the existing scholarly work on covert action. Covert action was defined as 'an activity or activities … to influence political economic or military conditions abroad where it is intended that the role of the … Government will not be apparent or acknowledged publicly'.[5]

The definition of cyber offensive operations that was used in this thesis was that offered by US government, and states that these operations are designed to produce an effect in the real world.[6] This then separates cyber offensive operations from cyber intelligence. Cyber offensive operations are, according to the US government, conducted by 'the manipulation, disruption, denial, degradation, or destruction of computers, information or communication systems, networks, physical or virtual infrastructure controlled by computers or information systems, or

[1] Daugherty, 'The Role of Covert Action', p. 283
[2] Brantly, 'Cyber Action by State Actors', 465-484
[3] Lowenthal, *Intelligence*, Seventh Edition, pp. 249-273.
[4] Ibid., pp. 249-273.
[5] Ibid., p. 249
[6] Edward Snowden Document, US Government, 'Presidential Policy Directive/PPD-20 Subject US Cyber Operations Policy', n.d., p. 3, edwardsnowden.com.

information resident thereon'.[7] These, the US argued, could be used to 'enable kinetic, information, or other types of operations'.[8] This is similar to the definition that GCHQ offered, but they define them simply as cyber effects operations.[9] These operations were conducted through the use of 'Destroy, Deny, Degrade, Disrupt, Deceive, Protect'.[10]

Using the understanding of what covert action is and what cyber offensive operations are, the thesis found that cyber offensive operations are covert action based on the fact that both types of activities are aimed at changing the behaviour of an adversary. Both types of activities will maintain a level of plausible deniability, and they are not war. From this, it can be concluded that overall a clear relationship between the activities exists based on what they are used for.

Using the definition of cyber offensive operations, the author then identified examples of cyber offensive operations. This was to allow for the author to analysis and to understand what types of activities these operations were being used for. When analysing these operations the author followed the argument of Kahn that actions between states can be seen to follow a hierarchy of violence.[11] Using this approach the author argued that there were six overarching ways that cyber offensive operations have been conducted.

The first type of cyber offensive operation that this thesis identified was propaganda. Willcox defined propaganda as 'the conscious or unconscious attempt by the propagandist to advance their cause through the manipulation of opinion, perception and behaviour of a target group'.[12] This thesis has found that states have used cyber offensive operations to conduct propaganda activities against both state and non-state actors. It argues that propaganda in cyber offensive operations can be seen to have taken place using human led operations. Human led operations are propaganda operations in which a human is used to control multiple online personas and is used to spread propaganda material. Further, this thesis has argued that states have conducted propaganda campaigns that are technology led. These operations are

[7] Ibid., p. 2.
[8] Ibid., p. 4.
[9] Edward Snowden Document, GCHQ, 'Full Spectrum Cyber Effects SIGINT as an Enabler for GCHQ's 'Effects' Mission', ca. 2010, p. 3, Snowden Surveillance Archive.
[10] Ibid., p. 3.
[11] Kahn, *On Escalation*, pp. 38-41
[12] Willcox, *Propaganda, The Press and Conflict*, p. 21.

conducted by states in such a way that a there is only minimal action needed from humans beyond programming. Finally, it has argued that it is not just through the use of social media that states have conducted cyber offensive propaganda operations, but states have also targeted online gaming systems to conduct propaganda campaigns. From this, it was clear that states have used cyber offensive operations to conduct propaganda operations.

This thesis also argued that states have the capacity to use cyber offensive operations to conduct direct counter propaganda operations. It argued that these operations should be seen as different to propaganda operations as direct propaganda operations are aimed at taking control of a target's own propaganda network and using it against the target. This type of activity was demonstrated to have taken place when the British conducted such an operation against Al Qaeda in Operation CUPCAKE. In this operation, the British took control of the of an online Al Qaeda magazine and changed the propaganda that was contained within this magazine. In addition, this thesis also demonstrated that groups that have been linked to the Syrian government have targeted a number of news agencies in similar fashion.[13] In this way, this thesis argued that direct counter propaganda is a form of cyber offensive operations.

This thesis found that cyber offensive operations have also been used to conduct political cyber offensive operations. It argued that political cyber offensive operations have been used to conduct defacement operations, where a state will deface the website of an organisation belonging to another state, or they could deface a non-state actor's website. This was illustrated through the example of a number of South Korean websites being defaced with pro-Kim Jong-un statements. Further, it illustrated that states have the ability to stop government websites from working. An example for this type of activity can be seen to have taken place in 2007 when a number of Estonian websites were stopped from working. It argued that states have the ability to conduct operations in which they leak information about either a person directly connect to a state, a state organisation, or even, a non-state actor such as a terrorist organisation. In these operations, a state will look to publish information that

[13] Andrew Griffin, 'Syrian Electronic Army hacks global websites including The Independent', *The Independent*, first published on 27.11.2014, http://www.independent.co.uk/life-style/gadgets-and-tech/news/syrian-electronic-army-hacks-global-websites-including-the-independent-9887176.html, last accessed on 18.03.2015.

is damaging so as to cause a target's own domestic population to question a state, a person, a private business or a terrorist organisation. It demonstrated that states have the ability to conduct political cyber offensive operations, in such a way, that a state aims for a population to know that they conducted the operation, but that it cannot prove that it was conducted by them. The example of this type of activity was the targeting of *Sony Pictures Entertainment* by North Korea in 2014. In this operation a state would target a particular non-state actor so that it has the maximum political impact. This thesis also argued that states have used cyber offensive operations to conduct resentment campaigns. In these operations, a state placing information or fake documents that are meant to target a particular section of the targets state population or even a department of government, with the hope of creating a situation where a marginalised group will rise up and either create greater problems for a state or even overthrow a state. This can be seen to have taken place where the Russians spread information about an unarmed black person being killed by police in, what it could be argued, was aimed at creating large demonstrations or even riots.[14] It illustrated that it may be possible in the future for states to conduct operations in which they try to change the outcome of an election or cause people to question an election result. This type of operation would likely only work in a number of places that have online voting. Finally, the thesis examined the Russian involvement in the US presidential election. It illustrated how the operations took place and the alleged goals of the operations. In these ways, it argued that there were six ways that political cyber offensive operations can take place.

This thesis discovered that states could conduct cyber offensive operations for an economic purpose. It found that these types of operations are more likely to be directed against non-state actors such as private businesses and terrorist organisations. By targeting private businesses a state could affect another state's economic powers but do so in an indirect manner. It argued that there were seven ways that economic operations can be seen to take place. The first is denial of service operation. This is where a state targets online banking systems and shuts off access to these services for clients. It also argued that states could use cyber offensive operations where they

[14] Adrian Chen, 'The Agency From a nondescript office building in St. Petersburg, Russia, an army of well-paid "trolls" has tried to wreak havoc all around the Internet — and in real-life American communities.' *The New York Times Magazine*, first published on 02.06.2015, http://www.nytimes.com/2015/06/07/magazine/the-agency.html?smid=nytcore-ipad-share&smprod=nytcore-ipad&_r=0, last accessed on 03.06.2015.

remove money from a particular individual or group account. This could be of use to target a state's leadership, or terrorist organisations. It also argued that states could use cyber offensive operations to target business accounts. It argued that this was seen to have been an option by GCHQ and it could be used to affect other businesses beyond the account that was being targeted. This thesis also found that states could use cyber offensive operations to stop a business from working, creating an economic effect. It also argued that if a state conducted a cyber offensive operation in a particular way, it would be possible that the operation itself could have an economic effect. This would be where because of leaking of information, people begin to question a company and switch to a different company. It argued that economic cyber offensive operations could be used in such a way that they could remove money from a banks own accounts or even target states reserve accounts. This was termed a cyber heist. Finally, this thesis argued that economic cyber offensive operations could be used in such a way that they spread damaging information about an organisation so as to cause an economic effect. In this way, this thesis has argued that there are seven forms of economic cyber offensive operations.

The final forms of cyber offensive operations that this thesis identified were high-end operations. This author chose not to term these as sabotage, as some authors chose to. This is because using cyber offensive operation to sabotage systems is used in a number of operations such as economic operations.

It argued that cyber offensive operations could be used to target individuals. It has argued that due to the fact that these tools were stated by GCHQ to have been withheld unless specifically authorised in the case of the British, targeting individuals should be seen as a high-end operation.[15] This author also argued that a state would target a particular individual only when this person was seen as highly important. This shows that it is a high level operation. The next form was stopping government services from working. This thesis argued that, due to the level of violence of this operation, it must be seen as a high-end operation as it could, theoretically, end up causing a government to collapse. This thesis illustrated that, in the future, cyber offensive operations might be used to assassinate a person. Although this author argued that it could be used, at present, it is unlikely due to the difficulties in

[15] Edward Snowden Document, GCHQ, 'JTRIG Tools and Techniques', Snowden Surveillance Archive.

conducting such an operation, it is possible in the future to be a form of operation that states can use. Finally, this thesis argued that states could use cyber offensive operations to target critical national infrastructure such as power stations as was the case in the Ukraine. It also demonstrated this by looking at the cyber offensive operation launched against the Iranian nuclear program. In these ways, this author has argued that there are five high-end cyber offensive operations.

The thesis also addressed the nature and the types of covert action. Johnson and Lowenthal argued that covert action follows a hierarchy of violence.[16] This violence was originally from the work of Kahn who argued that actions between states follow a level of violence. This author firstly addressed what covert action is. It found that there was general agreement within the academic literature about what covert action is used for and how it is defined. Covert action was defined as 'an activity or activities … to influence political economic or military conditions abroad where it is intended that the role of the … Government will not be apparent or acknowledged publicly.'[17] The author uncovered that the forms of covert action are debated. Some argue that there are three ways of conducting covert action: propaganda, political, paramilitary.[18] Others argued that there are five ways that covert action can be conducted: propaganda, political, economic, coup d'état, and paramilitary.[19]

This author illustrated five types of covert action: propaganda, military deception, political, economic, and paramilitary. The author broke down the forms for covert action in this way for a number of reasons. Political activities defined as a broad term of operations where the aim is to affect the power and policies of another country.[20] From this, the author felt that a coup was just a highly successful form of political activity. Secondly, this author wanted to highlight the differences between political and economic operations. Although these two operations are closely connected, they should be treated as different.

The study then looked to demonstrate the typology of covert action by providing examples of it use. This was to clarify how covert action has been used and

[16] Johnson, *Secret Agencies*, pp. 60-88; Lowenthal, *Intelligence,* Seventh Edition, pp. 249-275
[17] Lowenthal, *Intelligence*, Seventh Edition, p. 249.
[18] Rositzke, *The CIA's Secret Operations*; Gregory Treverton, *Covert Action*.
[19] Lowenthal, *Intelligence*, p. 169f.
[20] Rositzke, *The CIA's Secret Operations*, p. 185.

the forms of activities that make up covert action. It has demonstrated the use of propaganda. This included the use of radio propaganda campaigns, with Radio Free Europe and Radio Liberty. It was argued by Roy Godson, that one of the most successful propaganda campaigns was the US support of the Solidarity movement in Poland during the 1980s.[21] In addition, it argued that propaganda campaigns have not only been directed against state actors but also have been used against non-state actors. For example, the British government used their propaganda machinery to 'overtly and covertly, to blacken the IRA'.[22] These operations were conducted in such a way that it was hoped that it could not be proved to have been the British. From this they were argued to be covert action.

It demonstrated the use of political covert action through the used of including the use of agents of influence such as Stevenson who worked for the British to try and persuade the US to get involved in the Second World War.[23] This type of activity also includes helping to win a number elections in Chile where the US helped to advise on winning a campaign. [24] It also argued that political covert action has been used in such a way that information would be leaked which would affect a particular person. Finally, it demonstrated the highest level of political covert action being aimed at overthrowing a particular government. This has been used in the case of the joint US-UK action against the Premier of Iran Mossadeq.[25]

This study also looked at the economic covert action. The British developed a plan in which an economic covert action would be used to target the Soviet bloc. The operations that were discussed were to increase unrest in the labour force either by increasing the tensions that were felt towards communism or even play into national hostilities that countries felt towards each other including friction between Polish and Czech.[26] They also looked at targeting the economies by denying equipment that would, if it were provided, help the economies.[27] In also used the case of the CIA's

[21] Godson, *Dirty Tricks and Trump Cards*, p. 152.
[22] Aldrich and Cormac, *The Black Door*, p. 174.
[23] West (ed), *British Security Conordination*, p. 16f.
[24] United States, Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, 'Church Committee Covert Action in Chile 1963-1973 Staff report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities', p. 9.
[25] Aldrich, *The Hidden Hand*, p. 473.
[26] TNA, CAB 134/3, 'Official Committee of Communism Overseas' The Vulnerability of Satellite economy to external and internal pressure report prepared by the Ministry of Defence JIB and Foreign Office EID B.14/G.3, pp. 1-3.
[27] Ibid, pp. 1-3.

involvement in Guatemala in 1953-1954 in which private companies played a supporting role to the US' covert action campaign. It was noted that they planned to use an 'already cleared group of top ranking American businessmen in New York City' to create shortages of imports and cut the level of exports that Guatemala were able to conduct.[28] These operations had been used to affect the economies of the target countries.

Finally, the study addressed paramilitary of covert action. Under this form of covert action, there are assassinations. Further, it found that states have used covert action to supply arms and support to guerrilla groups such as the CIA's involvement Guatemala in 1952-1954 the operations can be much bigger. The CIA aimed to give enemies of the communist government in October 1952 around '250 rifles, 380 pistol, 64 machine guns and 4500 grenades'.[29] This form of covert action can be very large for example in 1961 the US had been involved in the Bay of Pigs operation. The Bay of Pigs operation involved the training of around 600-700 Cuban exiles to landings in Cuba in the hopes that this force could take control of Cuba.

Using the comparative methodology, this thesis was able to demonstrate in chapters two, three, and four that the types of cyber offensive operations and the forms of covert action all belong to the activities of covert action identified by covert action scholars. For example, the use the propaganda campaigns during the Cold War are directly comparable to those social media campaigns that states have conducted using cyber offensive operation. The political campaigns have a cyber equivalent. Economic cyber covert actions are comparable to the activities that were seen in chapter two. Finally, it argued that the use of high-end cyber offensive operations, are comparable to those of paramilitary activities. This is because if a foreign power trained a force to target a power station, this would be a paramilitary operation. It is possible, although this study argued that for the time being it is unlikely, that cyber offensive operations could be used to assassinate a person. In these ways, the author has argued cyber offensive operations are covert action.

The author argued that cyber offensive operations should be termed covert action achieved through cyber means. This was because, the actions meet the criteria of being an unacknowledged use of force. Even though states have, as Rid and

[28] Nick Cullather, *Secret History*, p. 41.
[29] Cullather, *Secret History*, p. 29f.

Buchanan argued, ways to attribute cyber offensive operations.[30] However, the ability to argue that it is highly likely that a state conducted an operation, is not the same as proof – as such, cyber offensive operation achieved the notion of an unacknowledged use of force. Further, it is clear that the use of cyber offensive operations is aimed at changing the behaviour of a foreign power. This was clearly demonstrated in the case of the Stuxnet operation against Iran. Finally, the actions fall outside of the actions of being war. In all of these ways, they are covert action.

Although, some covert action literature sees cyber offensive operations merely as another form of covert action,[31] this study argued against this idea. This is because of the fact that cyber means of achieving covert action can be used to conduct all the forms of covert action and not just one type. Further, this author has argued that cyber means should be treated a different to traditional covert action because they can be used together. For example, Operation Orchard where Israel launched a campaign to take down a Syrian air defence network so that Israel could destroy a nuclear facility, demonstrates the use of traditional and cyber means of covert action together.[32] In addition, online HUMINT may be used to begin a traditional covert action campaign. This is because after a particular intelligence agency has made contact with a particular person or group and cultivated a relationship this person or group could then be used to conduct traditional covert action. This could be through using the person to spread news stories; it could be through political activities; or it could be through paramilitary operations.

However, although these activities clearly are covert action, the author argued that the existing literature on covert action fails to address this properly. For example Daugherty and Brantly only see covert action achieved through cyber means as being used for one type of operation.[33] Yet, this is clearly not the case. Further, Lowenthal, only see three ways that covert action via cyber means could be used: propaganda, political, and economic.[34] This was not the case. It can achieve all forms of covert action.

[30] Rid and Buchanan, 'Attributing Cyber Attacks', 4-37.
[31] Daugherty, 'The Role of Covert Action', p. 283.
[32] Rid, *Cyber War Will Not Take Place*, p. 42.
[33] Daugherty, 'The Role of Covert Action', p. 283; Brantly, 'Cyber Action by State Actors', 465-484.
[34] Lowenthal, *Intelligence*, Seventh Edition, p. 256f.

Further, this author has argued that Lowenthal in his attempts to allow for covert action achieved through cyber means to be included in the traditional study of covert action has created a flawed ladder of escalation.[35] The ladder of escalation was created to allow researchers to understand in, Lowenthal's words, the violence of the types of covert action activities. Lowenthal's model makes the argument that a sabotage operation would be less violent in terms of action than a paramilitary operation. However, as was shown with the Russian covert action using cyber means against the Ukrainian power plants in 2015-2016, it can be used to affect a huge number of people. From this, there was a need to readdress the covert action theory of the ladder of escalation. The author's ladder also went further than Lowenthal's in that in broke down the types of activities into smaller parts. This allows for others to understand that even within a type of activity there are different levels of violence to the actions. The author's ladder also coded the actions to demonstrate the ways that traditional covert action and covert action achieved via cyber means could be used together for the same type of activity. In these ways, the author has clearly questioned and adapted the traditional theory of covert action to allow for the effective inclusion of covert action achieved through cyber means.

Using the fact that cyber offensive operations are covert action but those that are achieved through cyber means, the author investigated the issues that this creates for states when organising a covert action. Using historical examples there is clear evidence of some of these issues. This argument was demonstrated by addressing the fact that when states have had more than one organisation conducting covert action they inevitable run into each other. From the British experience, SOE and PWE did not function effectively as they could because of the fact that the operations were interlinked but that they were two separate organisations. From this, there is clearly a danger of an uneasy relationship between covert action and covert action by cyber means, due to the fact that there are at least, in both the UK and the US, two different organisations that can argue for control of the operations.

In addition, this thesis attempted to demonstrate the dangers of splitting the cyber means of conducting covert action from intelligence as appears to be the aim in the US by removing US Cyber Command from the dual hatted control of the Director of the NSA. It was argued by Rostizke that due to the official split in the covert action

[35] Ibid., p. 257.

and intelligence in the US from 1948-1952, there was featured duplication and confusion.[36] It was argued that when the British did the same by splitting SOE from SIS, there were issues. From this, it is clear that there is a real danger that by dividing cyber means of conducting covert action away from cyber intelligence the two parts will not work well together based on the historical examples.

Finally, this study dealt with the ethics of the use of covert action both in the traditional sense and covert action achieved through cyber means. The ethics of these activities were assessed against the six jus ad bello principles of JWT: Just cause, just intentions, proper authority, reasonable chance of success, last resort, proportionality as well as the jus in bellum principle of civilian immunity. The author found that the ethics of these operations must be theorised in relation to what these operations actually are. It found that part of the problem of discussing the ethics of covert action using cyber means is that the focus has been on the use of cyber offensive operation as being cyber war.[37]

Taking the approach of covert action, the author found that covert action achieved through cyber means does face minor new ethical issues. The most notable of these was the fact that in terms of assessing the criteria of reasonable chance of success, there is a danger that the use of covert action achieved through cyber means may create, as Singer argued, a Pandora's box effect.[38] The argument is if a state conducts a novel activity then others will attempt to do the same. However, this thesis has argued that although it is an issue that clearly states should be aware of, it is likely that this will diminish overtime. Overall, although there were further minor ethical issues that states should address in relation to covert action achieved through cyber means. Some of these are related to the organisational structure of covert action. What should be remembered is that it is important for states such as the US and the UK to use covert action via cyber means ethically. This is because, as Omand argued, that what one state claims in relation to intelligence others can claim as well.[39] From this, there is a clear basis to argue that states should use covert action achieved through cyber means ethically.

---

[36] Rositzke, *The CIA's Secret Operations*, p. 150
[37] Dipert, 'The Ethics of Cyberwarfare', 384-410; Beard, 'Just War, Cyberwar, and Cyber Espionage'; Arquilla, 'Ethics and Information Warfare'; Lucas, *Ethics and Cyber Warfare*.
[38] Singer, 'Stuxnet and its Hidden Lessons on the Ethics of Cyber Weapons', 86.
[39] Omand, in Omand and Phythian, 'Ethics and Intelligence: A Debate', 53.

In all of these ways, the study has revisited the traditional ideas of covert action to understand and establish its relationship to cyber offensive operations. The two types of activities are directly related and cyber offensive operations should be seen as being covert action achieved through cyber means.

Further Research

It is likely that, as more evidence becomes available, there will be need to review and revise some of the conclusions and evidence in this thesis. Firstly, it is highly likely that there will be more examples of the use of covert action achieved through cyber means. It could be that the types of operations that were argued to be theoretical in this thesis may, in fact, take place, if they have not already done so. This author believes this would most likely occur in relation to political activities in that a covert action using cyber means may target the voting system to actually change tallies. Whether this operation is conducted to change the election so no one notices or if it is done in such a way that the aim is to cause a crisis in democracy it does not matter. It will mean that there will be other examples of covert action achieved through cyber means that will allow for a clearer understanding.

A further area of work may be that Edward Snowden and others may leak more documents that will provide more information on the relationship between cyber offensive operations and covert action. It was estimated that Edward Snowden stole around 1.5 million documents. This means that there has only been a small number that have actually been leaked into the public domain. If this is the case then it will allow for further research into the types of activities that states have conducted.

In addition, as of yet, the organisational system for covert action in relation to cyber means is not yet clear. For example, in the case of the US Cyber Command it was, at the time of writing this, still commanded by the director of the National Security Agency. Although, this thesis has argued that splitting covert action away from intelligence, based on historical examples, is not an easy task and that it may not even be wise, it has been argued that it is a question of when not if for the split. This means that in a few years, researchers will be able to assess the effectiveness of this system.

Further, researchers will be able to have access to more documents about cyber intelligence and covert action achieved through cyber means. In the case of US, their system of FOI seems to have allowed for some documents to have already reached the public domain. In the case of the UK, it is likely that from around 2030 based on the Twenty Year rule for historical documents, Cabinet Office, Foreign Office, and other UK papers about covert action by cyber means should start to enter the public domain. Researchers, should see the benefit of using FOIA requests as was argued by Murphy and Lomas.[40] Using FOIA and the documents that are released by the British government, future researchers into covert action achieved through cyber means with have more official documents to use in their studies to them to test the finding of this thesis.

It is also hoped that, at some point in the future, a complete comparison between the information that has been leaked by Edward Snowden and others with official government documents. This would allow for a greater understanding of the information that is contained within the leaks. It would also mean that researchers in the future would be able to use leaks to fill in the blanks of official documents after they have been redacted. Future researchers will be able to test the notion of cyber war not being a real event against future operations. It is hoped that this research will allow for, as Rid argued, the move away from the cyber war terminology towards an understanding of cyber activities in the wider context of covert action.

[40] Murphy and Lomas, 'Return to Neverland', 273-87.

Bibliography

Primary Sources: The Edward Snowden Documents (All accessed via Snowden Surveillance Archive, or Edwardsnowden.com)

Communication Security Establishment Canada, 'CASCADE Joint Cyber Sensor Architecture Presentation'.

Communication Security Establishment Canada, 'CSEC Cyber Threat Capabilities SIGINT and ITS: an end-to-end approach presentation'.

GCHQ, 'Cyber Offensive Session: Pushing the Boundaries and Actions Against Hacktivism', ca. 2012.

GCHQ, 'Full Spectrum Cyber Effects SIGINT as an Enabler for GCHQ's 'Effects' Mission', ca. 2010.

GCHQ, 'Psychology A New Kind of SIGDEV Establishing the Human Science Operations Cells'.

GCHQ, 'SIGDEV Conference 2012 Cyber Intergration "The art of the possible"', added reporting from NBC News, Snowden Files: British Spies Used Sex and 'Dirty Tricks', ca. 2012,

GCHQ, 'What's the Worst That Could Happen', March 2010.

GCHQ, Human Systems Group, Information Management Department DSTL Behavioural Science Support for JTRIG's (Joint Threat Research and Intelligence Group's) Effects and Online HUMINT Operations', 10 March 2011.

GCHQ, JTRIG, 'Operational Highlights' August 2009

Mission Capabilities Presentation, 'HIDDENSALAMANDER Alerting and Characterization of Botnet Activity in TURMOIL', no date given.

National Security Agency, 'Exceptionally Controlled Information (ECI)', 12 September 2003.

National Security Agency/ Central Security Service 'Topic: Exploiting Terrorist Use of Games & Virtual Environments', 08.01.2007.

National Security Agency/ Central Security Service and US Strategic Command Joint Functional Component Command-Network Warfare (JFCC-NW) 'National Initiative Protection Program – Sentry Eagle', Draft reference number 20310524, no date given.

National Security Agency/ Central Security Service, '2010 SIGINT Development Conference SIGDEV: Discovery in the Cyber Age QUANTUMTHEORY' no date given

National Security Agency/ Central Security Service, 'DEFIANTWARRIOR and the NSA's Use of Bots', 24.04.2010.

National Security Agency/ Central Security Service, 'Iran—Current Topics, Interaction with GCHQ', no date given.

National Security Agency/ Central Security Service, 'S3285/Intern Projects', no date given.

National Security Agency/ Central Security Service, 'SIGDEV (SIGINT Development) 'Cases of Integrated Cyber Operation Techniques', no date given.

National Security Agency/ Central Security Service, 'Sir Iain Lobban, KCMG, CB Director, Government Communications Headquarters (GCHQ)' 30 April 2013 - 1 May 2013 GEN A Hosted Dinner: 30 April 2013//1830Hrs - Quarters

GEN A Hosted Discussion 01.05.2013, Accompanying Senior James M. Cusisk, Director Foreign Affairs,
National Security Agency/ Central Security Service, 'SNIPs of SIGINT Monthly June 2012', no date given.
National Security Agency/ Central Security Service, 'The ROC: NSA's Epicentre for Computer Network Operations', O8 January 2007.
National Security Agency/Central Security Service, 'Memo: Islamic Radicalization', 03 October 2013.
National Security Agency/Central Security Service, 'SIGINT Strategy 2012-2016' published as an internal document on 23.02.2012.
National Security Agency/Central Security Service, 'Visit Precis Between Bernard Barbier the Technical Director Directorate for External Security France and Patric Pailloux', 12.04.2013.
Naval Information Operations Command Maryland, 'NIOC Maryland Advanced Computer Network Operations Course Presentation', No data given.
No author given, 'Computer Network Operations: GENIE', no date given.
Office of the Director of National Intelligence, 'Congressional Budget Justification, Volume I, FY 2013, National Intelligence Program Summary', February 2012.
Office of the Director of National Intelligence, 'Quadrennial Intelligence Community Review Final Report', April 2009.
SAIC, From Science to Solution, 'Games: A look at Emerging Trends, Users, Threats and Opportunities in Influence Activities', no date given.
US Government, 'Presidential Policy Directive/PPD-20 Subject US Cyber Operations Policy', no date given.

Primary Sources: Leaked Documents, other than Edward Snowden

Steele, Christopher, 'US Presidential Election: Republican Candidate Donald Trump's Activities in Russia and Compromising Relationships with the Kremlin', Company Intelligence Report 2016/080, accessed via https://www.documentcloud.org/documents/3259984-Trump-Intelligence-Allegations.html, last accessed 30.06.2017
Wikileaks Files, 'Macron Campaign Emails'
Wikileaks Files, Sony Files
Wikileaks Files, Vault 7

Primary Sources: Hearings, Debates, Public Interviews, and Speeches

Aspen Security Forum, 'Beyond The Build: Leveraging The Cyber Mission Force Aspen', David Sanger *The New York Times* and Michael Rogers, Director National Security Agency, Commander, U.S. Cyber Command July 23, 2015
Aspen Security Forum, 'Mission Possible 2017', Moderator David Ignatius, Speakers Admiral Mike Rogers, Director of the NSA and US Cyber Command, and Robert Hannigan, former Director of GCHQ.
HM Government, Michael Fallon, 'Defence Secretary's speech at Cyber 2017 Chatham House Conference', 27.06.2017, https://www.gov.uk/government/speeches/defence-secretarys-speech-at-cyber-2017-chatham-house-conference, last accessed on 28.06.2017.

House of Commons, 'Aleppo/Syria: International Action', 13 December 2016 Volume 618 Emergency debate (Standing Order No. 24) column 652-654 https://hansard.parliament.uk/Commons/2016-12-13/debates/16121344000001/AleppoSyriaInternationalAction#contribution-935FBA3F-3657-4CAE-9743-5A488A0204FE

United States, House Permanent Select Committee on Intelligence, 'Hearing On Russian Active Measures Investigation', *Political Transcript Wire*, 20.03.2017

United States, Senate Armed Services Committee, 'Hearing To Receive Testimony On Cyber Strategy And Policy', 2.03.2017.

United States, Senate Armed Services Committee, 'Hearing To Receive Testimony On Cyber Policy, Strategy, And Organization', 11 May 2017.

United States, Senate Select Committee on Intelligence, 'Hearing On Russian Active Measures Investigation', *Political Transcript Wire*, 20 March 2017.

United States, Senate Select Committee on Intelligence, 'Hearing On Russian Interference in 2016 Election, Panel 1', 21 June 2017.

United States, Senate Select Committee on Intelligence, 'Hearing On Russian Intelligence Activities', 10 January 2017.

United States, Senate Select Committee on Intelligence, 'Open Hearing: FISA Legislation', 26 September 2013.

United States, Senate Select Committee on Intelligence, 'Open Hearing: Russian Intervention in European Elections', 28 June 2017.

Private Organisation Reports

Albright, David, Brannan, Paul, and Walrond, Christina, 'Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report', *Institute for Science and International Security*, 16 February 2011.

Falliere, Nicolas, Murchu, Liam, O., and, Chien, Eric, 'W32.Stuxnet Dossier Version 1.4', *Symantec Security Response*, February 2011.

Kaspersky Lab, 'Chasing Lazarus: A Hunt for the Infamous Hackers to Prevent Large Bank Robberies', https://www.kaspersky.com/about/press-releases/2017_chasing-lazarus-a-hunt-for-the-infamous-hackers-to-prevent-large-bank-robberies, 03 April 2017

Samani, Raj, and, Beek, Christiaan, 'Updated BlackEnergy Trojan Grows More Powerful' *McAfee*, 14 January 2016.

Scott, James, and Spaniel, Drew 'Hacking Elections is Easy! Part 1: Tactics, Techniques, and Procedures' *Institute for Critical Infrastructure*, September 2016

Scott, James and Spaniel, Drew, 'Hacking Elections is Easy! Part 2: Psst! Wanna Buy a National Voter Database? Hacking E-Voting Systems Was Just the Beginning' *Institute for Critical Infrastructure*, September 2016

Published Primary Sources: Diaries, Memoirs, and Autobiography

Colby, William E., with Forbath, Peter, *Honorable Men: My Life in the CIA*, (New York: Simon & Schuster, 1978).

Masterman J.C., *The Double-Cross System The Incredible True Story of how Nazi Spies Were Turned into Double Agents*, (Guilford: Lyons Press, 2012).

Published Primary Sources: The National Archives (UK)

CAB 81 – War Cabinet and Cabinet: Committees and Sub-committees of the Chiefs of Staff Committee: Minutes and Papers

CAB 134 – Cabinet: Miscellaneous Committee: Minutes and Papers (DO, D, and DC Series)

CAB 301—Cabinet: Organisation And Funding Of British Intelligence: General

DEFE 28 – Ministry of Defence: Directorate of Forward Plans: Registered Files

Published Primary Sources: The National Security Archive (US)

Department of Defense, Instruction S-3325.10, Subject: Human Intelligence (HUMINT) Activities in Cyberspace, June 6, 2013. Secret/Noforn. http://nsarchive.gwu.edu/dc.html?doc=2692127-Document-19 last accessed on 20.07.2017

Donald N. Wilber, CIA, Clandestine Services History, Overthrow of Premier Mossadeq of Iran: November 1952 - August 1953, March 1954

USCYBERCOM to CDRUSACYBER, Subj: CYBERCOM FRAGORD 01 to TASKORD 16-0063 To Establish Joint Task Force (JTF)-ARES to Counter the Islamic State of Iraq and the Levant (ISIL) in Cyber Space, May 5, 2016. Secret//Rel to USA, [Redacted].

Published Primary Sources: Other Archives

US Government, 'Scope of CIA Activities under the Nicaragua finding September 19', 1983 https://www.brown.edu/Research/Understanding_the_Iran_Contra_Affair/documents.php.

Published Primary Sources: Transnational Organisations Documents

Galeotti Mark, 'Putin's Hydra: Inside Russia's Intelligence Service' *European Council on Foreign Relations*, ECFR/169 1-19.

International Court of Justice, 'Case Concerning Military and Paramilitary activities in and Against Nicaragua 1986'.

NATO STRATCOM, 'Internet Trolling As A Tool Of Hybrid Warfare: The Case Of Latvia', no date given.

UN Charter Chapter VII http://www.un.org/en/documents/charter/chapter7.shtml last accessed on 26.01.2015

UN Charter, Chapter I http://www.un.org/en/documents/charter/chapter1.shtml last accessed on 27.11.2014

United Nations 'Definition of Aggression 3314 (XXIX) 2319 Plenary Meeting', 14.12.1974

United Nations Security Council, 'Letter dated 7 September 2015 from the Permanent Representative of the United Kingdom of Great Britain and Northern Ireland to the United Nations addressed to the President of the Security Council' http://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_2015_688.pdf

Published Primary Sources: United Kingdom Government

HM Government, 'A Strong Britain in an Age of Uncertainty: The National Security Strategy', October 2010.

HM Government, 'Criminal Finances Act 2017, Chapter 22'.

HM Government, 'Government Response to the Intelligence and Security Committee's Annual Report 2011-2012', November 2012.

HM Government, 'Intelligence Service Act 1994'.

HM Government, 'Justice and Security Act 2013, Chapter 18'.

HM Government, 'National Cyber Security Strategy 2016-2021', published 1 November 2016.

HM Government, 'National Security Strategy and Strategic Defense and Spending Review: A Secure and Prosperous United Kingdom', November 2015.

HM Government, 'The UK Cyber Security Strategy Protecting and promoting the UK in a digital world', November 2011.

HM Government, Cabinet Office, 'Progress against the Objectives of the National Cyber Security Strategy', December 2012.

HM Government, Cabinet Office, 'Progress against the Objectives of the National Cyber Security Strategy', December 2013.

HM Government, Cabinet Office, 'The National Cyber Security Strategy Our Forward Plans', December 2013.

HM Government, Cabinet Office, 'The UK Cyber Security Strategy Report on Progress and Forward Plans', December 2014.

HM Government, Centre for the Protection of National Infrastructure, https://www.cpni.gov.uk/critical-national-infrastructure-0

HM Government, Intelligence and Security Committee of Parliament, 'Annual Report 2011–2012', July 2012

HM Government, Intelligence and Security Committee of Parliament, 'Annual Report 2012–2013' October 2013

HM Government, Intelligence and Security Committee of Parliament, 'Annual Report 2013-2014', 23 November 2014.

HM Government, Intelligence and Security Committee of Parliament, 'Privacy and Security: A Modern and Transparent Legal Framework', 12 March 2015.

HM Government, Intelligence and Security Committee of Parliament, 'UK Lethal Drone Strikes in Syria', 26 April 2017

HM Government, Ministry of Defence, 'Cyber Primer Development, Concepts and Doctrine Centre', December 2013.

HM Government, Ministry of Defence, 'How Defence Works Version 4.1', 30.09.2014.

HM Government, Ministry of Defence, 'Strategic Trends Programme Global Strategic Trends Out to 2045', Fifth Edition, 30 April 2014.

Silva, Desmond de, 'The Report of the Patrick Finucane Review Volume I', December 2012, (London: The Stationary Office)

Published Primary Sources: United States of America Government

Christie, Christopher J., U.S. Attorney, 'United States Department of Justice U.S. Attorney, District of New Jersey News', December 2013, https://www.justice.gov/archive/usao/nj/Press/files/pdffiles/Older/duro1213rel.pdf.

Erwin, Marshall Curtis, 'Covert Action: Legislative Background and Possible Policy Questions', *Congressional Research Service*, 10.04.2013.

Office of the Director of National Intelligence, 'Intelligence Community Assessment Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution', 6 January 2017.

Office of the Secretary of Defense, 'Military Power of the People's Republic of China A Report to Congress Pursuant to the National Defense Authorization Act 2000', published 2007.

United States, District Court Southern District of New York, 'United States v. Ahmad Fathi, Hamid Firoozi, Amin Shokohi, Sadech Ahmadzadegan a/k/a "Nitr0jen26, Omid Ghaffarinia a/k/a "PLuS, Sina Kissar, and Nader Saedi a/k/a "Turk Server", Indictment, no date given.

United States, District Court Southern District of New York, 'United States of America v Gery Shalon, Joshua Samuel Aaron, Ziz Orenstein.

United States, House Permanent Select Committee on Intelligence, 'Review of the Unauthorized disclosures of Former National Security Agency Contractor Edward Snowden' published 15.09.2016.

United States, Senate Committee on Armed Services, 'Hearing To Receive Testimony On Cyber Policy, Strategy, And Organization' 11.05.2017.

United States, Senate Select Committee on Intelligence, 'Study of the Central Intelligence Agency's Detention and Interrogation Program Approved December 13, 2012 Updated for Release April 3, 2014', Declassification Revisions, December 3, 2014, Executive Summary.

United States, Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, 'Alleged Assassination Plots Involving Foreign Leaders: An Interim Report of The Select Committee to Study Governmental Operations With Respect to Intelligence Activities United States Senate Together with Additional, Supplemental, and Separate Views.

United States, Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, 'Church Committee Covert Action in Chile 1963-1973, Staff report of the select committee to study governmental operations with respect to intelligence activities'.

United States, Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, 'Final Report Of The Select Committee To Study Governmental Operations With Respect To Intelligence Activities United States Senate Together With Additional, Supplemental, And Separate Views Intelligence Activities And The Rights Of Americans Book II'.

US Government, 'Intelligence Authorization Act, Fiscal Year 1991'.

US Government, 'International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World', May 2011.

US Government, 'National Defense Authorization Act For fiscal year 2017 Conference Report To Accompany S. 2943, 30 November 2016.

US Government, 'National Security Strategy', February 2015.

US Government, 'The National Intelligence Strategy of the United States of America 2014', no date given.

US Government, Department of Defence, 'Department of Defence Strategy for Operating in Cyberspace', July 2011.

US Government, Department of Defense, 'Department of Defense Directive O-3600.01 Information Operations' 14 August 2006.

US Government, Department of Defense, 'Fact Sheet: The Department Of Defense' Cyber Strategy, April 2015.
US Government, Department of Defense, 'National Defence Strategy' June 2008.
US Government, Department of Defense, 'The Department of Defense Cyber Strategy', April 2015.
US Government, Department of Defense, http://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy.
US Government, Department of Defense, http://www.defense.gov/News-Article-View/Article/643954/cybercom-chief-details-strategic-priorities-for-2016.
US Government, Department of Homeland Security, Critical Infrastructure Sectors https://www.dhs.gov/critical-infrastructure-sector.
US Government, Department of Homeland Security, Industrial Control Cyber Emergency Response ICS-CERT Alert (ICS-ALERT-13-164-01) Medical Devices Hard-Coded Passwords https://ics-cert.us-cert.gov/alerts/ICS-ALERT-13-164-01, first published 13 June 2013.
US Government, Department of Homeland Security, Industrial Control Systems Cyber Emergency Response Team Alert (IR-ALERT-H-16-056-01) Cyber-Attack Against Ukrainian Critical Infrastructure https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01, first published on February 25, 2016.
US Government, Department of State, Office of the Historian, 171. Note From the Executive Secretary of the National Security Council (Lay) to the National Security Council Washington, March 15, 1954. NSC 5412 Covert Operations Source: Eisenhower Library, Special Assistant to President for National Security Affairs Records, President's Papers. Top Secret. This directive was transmitted to the NSC under cover of a December 28 note from NSC Executive Secretary Lay. Lay stated that the President had approved the directive on the same date. Office of the Historian Department of State Foreign Relations Of The United States Foreign Relations Of The United States, 1950–1955, The Intelligence Community, 1950–1955 https://history.state.gov/historicaldocuments/frus1950-55Intel/d171 last accessed on 22.02.2017.
US Government, Department of State, Office of the Historian, NSC 10/2 292, National Security Council Directive on Office of Special Projects, https://history.state.gov/historicaldocuments/frus1945-50Intel/d292, last accessed on 20.10.2016.

Media Sources

Ackerman, Spencer, 'Snowden: NSA accidentally caused Syria's internet blackout in 2012', *The Guardian*, first published on 13.08.2014 http://www.theguardian.com/world/2014/aug/13/snowden-nsa-syria-internet-outage-civil-war, last accessed on 16.10.2014.
Arthur, Charles, 'Syrian Electronic Army' hacks Skype's Twitter and blog accounts'', *The Guardian*, first published on 02.01.2014, http://www.theguardian.com/technology/2014/jan/02/syrian-electronic-army-skype-twitter-blog, last accessed on 18.03.2015.
Baker, Peter, and, Erlanger, Steven, 'Russia Wields Aid and Ideology Against West to Fight Sanctions', *The New York Times*, first published on 07.06.2015, http://www.nytimes.com/2015/06/08/world/europe/russia-fights-wests-ukraine-sanctions-with-aid-and-

ideology.html?hp&action=click&pgtype=Homepage&module=first-column-region&region=top-news&WT.nav=top-news, last accessed on 08.06.2015.

Baldor, Lolita, C., 'New Pentagon strategy warns of cyberwar capabilities' *The Associated Press*, first published on 22.04.2015, http://m.apnews.com/ap/db_289563/contentdetail.htm?contentguid=jcHwulL6 , last accessed on 23.04.2015.

Baldor, Lolita, C., 'US to create independent military cyber command' *The Washington Post* first published 17.07.2017, https://www.washingtonpost.com/politics/federal_government/us-to-create-independent-military-cyber-command/2017/07/17/ec67a192-6abf-11e7-abbc-a53480672286_story.html?utm_term=.6636dc29c1a3, last accessed on 17.07.2017.

Ball, James, 'GCHQ has tools to manipulate online information, leaked documents show', *The Guardian*, first published on 14.07.2015, http://www.theguardian.com/uk-news/2014/jul/14/gchq-tools-manipulate-online-information-leak, Last accessed on 16.10.2014.

Baraniuk, Chris, 'Build 2016: Microsoft proposes helper bot boom', *BBC News*, first published on 30.03.2016, http://www.bbc.co.uk/news/technology-35927651, last accessed on 06.04.2016

Beaumont, Peter, 'International: Lab studies reveal extent of cyberwar against Iran', *The Guardian*, first published on 22.09.2012, Lexis Nexis.

Bennett, Cory, 'Bank hackers find haven in Putin's Russia', *The Hill*, first published on 17.02.15, http://thehill.com/policy/cybersecurity/233020-hackers-find-haven-in-putins-russia, last accessed on 18.02.2015.

Blue, Violet, 'eBay and PayPal UK domains hacked by Syrian Electronic Army', *ZDNET*, first published 02.02.2014, http://www.zdnet.com/article/ebay-and-paypal-uk-domains-hacked-by-syrian-electronic-army/ , last accessed 09.12.2015.

Bradbury, Danny, 'Should we hack the hackers? Western companies are being fleeced for hundreds of millions by cybercriminals. Is it time to give them a dose of their own medicine?', *The Guardian*, first published 09.03.2015, http://www.theguardian.com/technology/2015/mar/09/cybercrime-should-we-hack-the-hackers, last accessed on 09.03.2015.

Bugorkova, Olga, 'Ukraine conflict: Inside Russia's 'Kremlin troll army'', *BBC Monitoring*, first published on 19.03.2015, http://www.bbc.co.uk/news/world-europe-31962644 last accessed on 20.03.2015.

Capaccio, Tony, Lerman, David, and Strohm, Chris, 'Iran Behind Cyber-Attack on Adelson's Sands Corp., Clapper Says', *Bloomberg*, first published on 26.02.2015, http://www.bloomberg.com/news/articles/2015-02-26/iran-behind-cyber-attack-on-adelson-s-sands-corp-clapper-says, Last accessed on 27.02.2015.

Chen, Adrian, 'The Agency From a nondescript office building in St. Petersburg, Russia, an army of well-paid "trolls" has tried to wreak havoc all around the Internet — and in real-life American communities.', *The New York Times Magazine*, first published on 02.06.2015, http://www.nytimes.com/2015/06/07/magazine/the-agency.html?smid=nytcore-ipad-share&smprod=nytcore-ipad&_r=0, last accessed on 03.06.2015.

Chen, David, W., 'Man Charged With Sabotage Of Computers' *The New York Times*, first published on 18.02.1998,

http://www.nytimes.com/1998/02/18/nyregion/man-charged-with-sabotage-of-computers.html, last accessed on 07.05.2015.
Cooper Helene, 'China and U.S. engage in verbal face-off', *The New York Times*, first published on 09.04.2014, accessed via Nexis Business and News.
Corera, Gordon, 'NHS cyber-attack was 'launched from North Korea'', *BBC News*, first published on 16.06.2017, http://www.bbc.co.uk/news/technology-40297493 last accessed on 16.06.2017.
Corera, Gordon, 'Plaque unveiled for first MI6 chief Mansfield Cumming', *BBC News* first published on 31.03.2015, http://www.bbc.co.uk/news/uk-32126061 last accessed on 31.03.2015.
Cornwell, Rupert, 'Fears in the US of being outgunned in the vital propaganda wars by Russia, China - and even Isis - have prompted a rethink on overseas broadcasters' *The Independent*, first published on 19.04.2015, http://www.independent.co.uk/voices/fears-in-the-us-of-being-outgunned-in-the-vital-propaganda-wars-by-russia-china--and-even-isis--have-prompted-a-rethink-on-overseas-broadcasters-10186982.html, last accessed on 19.04.2015.
Crawford, Charles, 'Ukraine crisis: is NATO ready for Russia?' *The Telegraph*, first published on 31.07.2014, http://blogs.telegraph.co.uk/news/author/charlescrawford/, last accessed on 18.03.2015.
Crookes, Del, 'The internet is the new frontline as UK sets up army cyber-unit' *BBC News* first published on 31.01.2015, http://www.bbc.co.uk/newsbeat/31074227, Last accessed on 02.02.2015.
DARPA, 'Social Media in Strategic Communication (Smisc)', http://www.darpa.mil/Our_Work/I2O/Programs/Social_Media_in_Strategic_Communication_(SMISC).aspx , last assess on 28.05.2015.
Davenport, Christian, 'Why the Pentagon is wooing Silicon Valley (and the valley is playing hard to get)', *The Washington Post* first published on 23.04.2015, http://www.washingtonpost.com/news/checkpoint/wp/2015/04/23/why-the-pentagon-is-wooing-silicon-valley-and-the-valley-is-playing-hard-to-get/?tid=hpModule_04941f10-8a79-11e2-98d9-3012c1cd8d1e&hpid=z11, last accessed on 23.04.2015.
Dearden, Lizzie, 'US Government Hack: China Denies Responsibility for Cyber Attack That Stole Personal Details Of Four Million Employees' *The Independent*, first published on 05.06.2015, http://www.independent.co.uk/news/world/americas/us-government-hack-live-china-denies-responsibility-for-cyber-attack-that-stole-personal-details-of-four-million-employees-10298745.html?utm_source=Sailthru&utm_medium=email&utm_term=01%20Indy%20News%20List%2020150506&utm_campaign=Daily%20News%2020150605, last accessed on 08.06.2015.
Diebert, Ron, 'The Cyber Security Syndrome' *Open Canada.org*, first published on 25.12.2014, http://opencanada.org/features/the-cyber-security-syndrome/#.VHTwX9y6ROc.twitter, last accessed on 26.11.2014.
Dutta, Kunal, 'Isis is winning the digital propaganda war, says extremism expert' *The Independent* first published on 20.02.2015, http://www.independent.co.uk/news/world/middle-east/isis-is-winning-the-digital-propaganda-war-says-extremism-expert-10059200.html, last accessed on 20.02.2015.

Eilperin, Juliet, 'Obama announces initiatives to curb recruitment of terrorist groups', *The Washington Post*, first published on 18.02.2015, http://www.washingtonpost.com/politics/obama-announces-initiatives-to-curb-recruitment-of-terrorist-groups/2015/02/18/bc4800ca-b792-11e4-9423-f3d0a1ec335c_story.html?tid=hpModule_f8335a3c-868c-11e2-9d71-f0feafdd1394&hpid=z9 , last accessed on 19.02.2015.

Eisler, Peter, and Page, Susan, '3 NSA veterans speak out on whistle-blower: We told you so', *USA Today*, first published on 16.06.2013 http://www.usatoday.com/story/news/politics/2013/06/16/snowden-whistleblower-nsa-officials-roundtable/2428809/ , last accessed on 20.05.2013.

Elgin, Benjamin, and Michael, Riley, 'Now at the Sands Casino: An Iranian Hacker in Every Server', *Bloomberg*, first published on 12.12.2014, http://www.bloomberg.com/news/articles/2014-12-11/iranian-hackers-hit-sheldon-adelsons-sands-casino-in-las-vegas, last accessed on 27.03.2015.

Eremenko, Alexey, 'Is Russia's Cyberwar Heating Up Amid New Cold War?', *The Moscow Times*, first published on 26.11.2014, http://www.themoscowtimes.com/article.php?id=511873, last accessed on 24.03.2015.

Faiola, Anthony, 'Anti-Japanese Hostilities Move to the Internet; Chinese and South Korean Hackers Blamed for Digital Barrage Designed to Cripple Web Sites', *The Washington Post* first published on 10.05.2005, accessed via Lexis Business and News.

Fielding, Nick, and Cobain, Ian, 'Revealed: US spy operation that manipulates social media', *The Guardian*, first published on 17.03.2011, http://www.theguardian.com/technology/2011/mar/17/us-spy-operation-social-networks, last accessed on 17.04.2015.

Finkle, Jim, and Richwine, Lisa, 'Exclusive FBI warns of 'destructive' malware in wake of Sony attack' *Reuters*, first published on 02.12.2014, http://www.reuters.com/article/2014/12/02/us-sony-cybersecurity-malware-idUSKCN0JF3FE20141202, last accessed on 02.12.2014.

Fox-Brewster, Thomas, 'British Snoops GCHQ Openly Recruiting Hackers As Government Seeks More Surveillance Powers', *Forbes*, first published on 12.05.2015, http://www.forbes.com/sites/thomasbrewster/2015/05/12/gchq-courts-cyber-spies-as-snoopers-charter-reborn/, last accessed on 14.05.2015.

Freeze, Colin, and Dobby, Christine, 'NSA trying to map Rogers, RBC communications traffic, leak shows' *The Globe and Mail*, first published on 17.03.2015, http://www.theglobeandmail.com/news/national/nsa-trying-to-map-rogers-rbc-communications-traffic-leak-shows/article23491118/ last accessed on 18.03.2015.

Gallagher, Paul, 'Revealed: Putin's army of pro-Kremlin bloggers', *The Independent*, first published on 27.03.2015, http://www.independent.co.uk/news/world/europe/revealed-putins-army-of-prokremlin-bloggers-10138893.html, last accessed on 28.03.2013.

Gander, Kashmira, 'Kremlin to consider plans which could remove Russia from global Internet 'in an emergency'', *The Independent*, first published on 19.09.2014, http://www.independent.co.uk/news/world/europe/kremlin-to-consider-plans-which-could-remove-russia-from-global-internet-in-an-emergency-9745466.html , last accessed on 08.10.2014.

Gardham, Duncan, 'Britain prepares cyber attacks on rogue states' *The Daily Telegraph*, first published on 26.11.2011, accessed via Nexis Business and News.

Gardham, Duncan, 'MI6 attacks al-Qaeda in 'Operation Cupcake'' *The Daily Telegraph*, first published on 02.06.2011, http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/8553366/MI6-attacks-al-Qaeda-in-Operation-Cupcake.html, last accessed on 08.10.2014.

Goldman, Adam, and Craighill, Peyton, 'New poll finds majority of Americans think torture was justified after 9/11 attacks', first published 16.12.2014, https://www.washingtonpost.com/world/national-security/new-poll-finds-majority-of-americans-believe-torture-justified-after-911-attacks/2014/12/16/f6ee1208-847c-11e4-9534-f79a23c40e6c_story.html?utm_term=.5b5462b69329, last accessed 06.02.2017.

Goldstein, Matthew, 'Firms Wary of Breaches by Hackers, Not Terrorists' *The New York Times*, first published on 04.02.2015, accessed via Nexis Business and News.

Goodwin, Christopher, 'The spies who Hacked Him; The Flame computer virus that hit Iran shows cyberwarfare is being taken to ferocious levels, says Christopher Goodwin', *The Sunday Times*, first published on 03.06.2013 accessed via Nexis Business and News.

Gould, Joe, 'Former NSA Chief: Follow SOCOM Model for Cyber', *Defence News*, http://www.defensenews.com/story/defense-news/blog/intercepts/2015/04/17/keith-alexander-cyber-dod-aei/25951903/, last accessed on 20.04.2015.

Greenberg, Andy, ''Crash Override': The Malware That Took Down A Power Grid', *Wired*, first published 12.06.2017, https://www.wired.com/story/crash-override-malware/, last accessed on 12.06.2017.

Greenwald, Glenn, 'Obama orders US to draw up overseas target list for cyber-attacks', *The Guardian*, first published on 07.06.2013, http://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas, last accessed on 08.10.2014.

Griffin, Andrew, 'Angela Merkel's Instagram bombarded with abuse from Russian troll army', *The Independent*, first published on 07.06.2015, http://www.independent.co.uk/life-style/gadgets-and-tech/news/angela-merkels-instagram-bombarded-with-abuse-from-russian-troll-army-10303425.html, last accessed on 08.06.2015.

Griffin, Andrew, 'Syrian Electronic Army hacks global websites including The Independent', *The Independent*, first published on 27.11.2014, http://www.independent.co.uk/life-style/gadgets-and-tech/news/syrian-electronic-army-hacks-global-websites-including-the-independent-9887176.html, last accessed on 18.03.2015.

Harley, Nicola, 'British spies removed from operations after Russia and China crack codes to leaked Snowden files' *The Daily Telegraph*, first published on 14.06.2015, http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/11673533/British-spies-removed-from-operations-after-Russia-and-China-crack-codes-to-leaked-Snowden-files.html, last accessed on 15.06.2015.

Harris, Shane, 'China Reveals Its Cyberwar Secrets', *The Daily Beast*, first published on 18.03.15, http://www.thedailybeast.com/articles/2015/03/18/china-reveals-its-cyber-war-secrets.html, last accessed on 19.03.2015.

Harris, Shane, 'Report: Iranian Hackers Eye U.S. Grid', *The Daily Beast*, first published on 16.04.2015, http://www.thedailybeast.com/articles/2015/04/16/report-iranian-hackers-eye-u-s-grid.html?via=mobile&source=twitter, last accessed on 17.04.2015.

Harris, Shane, and Youssef, Nancy, A., 'U.S. Ratchets Up Cyber Attacks on ISIS', *The Daily Beast*, first published on 18.04.2016, http://www.thedailybeast.com/articles/2016/04/17/u-s-ratchets-up-cyber-attacks-on-isis.html?via=desktop&source=twitter, last accessed on 18.04.2016.

Hart, Kim, 'A New Breed Of Hackers Tracks Online Acts of War Hacktivists Update Their Mission', *The Washington Post* first published 27.08.2008, accessed from Nexis Business and News.

Harwell, Drew, and Nakashima, Ellen, 'China Suspected in Major Hacking of Health Insurer' *The Washington Post*, first published on 05.02.2015, http://www.washingtonpost.com/business/economy/investigators-suspect-china-may-be-responsible-for-hack-of-anthem/2015/02/05/25fbb36e-ad56-11e4-9c91-e9d2f9fde644_story.html?hpid=z1, last accessed on 06.02.2015.

Heather, Saul, 'London airspace shuts after 'computer failure'', *The Independent*, first published on 12.12.2014, http://www.independent.co.uk/news/uk/home-news/london-flights-disrupted-after-computer-failure-9921436.html, last accessed on 12.12.2014.

Hern, Alex, 'Syrian electronic army 'hacks' Independent, OK Magazine and NHL' *The Guardian*, first published on 27.11.2014, http://www.theguardian.com/technology/2014/nov/27/syrian-electronic-army-hacks-independent-ok-magazine-and-nhl, last accessed on 18.03.2015.

Hern, Alex, 'Wi-Fi on planes opens door to in-flight hacking, warns US watchdog', *The Guardian*, first published on 15.04.2015, http://www.theguardian.com/technology/2015/apr/15/wi-fi-on-planes-in-flight-hacking-us-government, last accessed on 15.04.2015.

HM Government, Secret Intelligence Service, Website, https://www.sis.gov.uk/our-mission.html, last accessed on 30.06.2017.

Holehouse, Matthew, 'Britain may broadcast Putin's financial secrets to Russian people', *The Daily Telegraph*, first published 10.03.2015, http://www.telegraph.co.uk/news/worldnews/europe/russia/11461163/Britain-may-broadcast-Putins-financial-secrets-to-Russian-people.html, last accessed on 10.03.2015.

Hopkins, Nick, 'UK developing cyber-weapons programme to counter cyber war threat', *The Guardian*, first published on 30.05.2011, http://www.theguardian.com/uk/2011/may/30/military-cyberwar-offensive, last accessed on 16.04.2015.

Jacobsen, Jeppe, T., 'The US and Europe Need to Coordinate Their Cyber Weapons' *Defense One*, first published 26.04.2017, http://www.defenseone.com/technology/2017/04/us-and-europe-need-coordinate-their-cyber-weapons/137346/?oref=d-channeltop, last accessed on 27.04.2017.

Jones, Sam, ''Victory' and 'defeat' things of past, says top UK general' , *The Finical Times*, first published on 17.02.2015, http://www.ft.com/cms/s/0/63e6e21c-b6d3-11e4-a33b-00144feab7de.html, last assessed on 17.02.2015.

Joye, Christopher, 'Australia launches cyber-weapons in global counter-terrorist operations', *The Australian Financial Review*, first published on 27.01.2015,

http://www.afr.com/p/technology/australia_launches_cyber_weapons_hR1B30qv3c6bYKJvquVzo, last accessed on 27.01.2015

Kauffmann, Sylvie, and Korneliusin, Stefan, 'From Islamism to Putin, Europe faces new threats – but can it unite to fight?', *The Guardian*, first published on 05.02.2015, http://www.theguardian.com/world/2015/feb/05/europe-threats-islamism-putin-security-terrorism-cyber-attacks, last accessed on 05.02.2015.

Kessler, Glenn, 'File the Bin Laden Phone Leak Under 'Urban Myths', *The Washington Post*, first published 22.12.2005, accessed via Nexis Business and News.

Kimberly, Dozier, 'Anti-ISIS-Propaganda Czar's Ninja War Plan: We Were Never Here', *The Daily Beast*, first published on 15.03.16 ,http://www.thedailybeast.com/articles/2016/03/15/obama-s-new-anti-isis-czar-wants-to-use-algorithms-to-target-jihadis.html, last accessed on 23.03.2016.

Kirk, Jeremy, 'Pacemaker Hack can deliver deadly 830 volt jolt', *Computerworld*, first published 17.10.2012, https://www.computerworld.com/article/2492453/malware-vulnerabilities/pacemaker-hack-can-deliver-deadly-830-volt-jolt.html, last accessed on 23.12.2015.

Knight, Ben, 'US considering pre-emptive cyberattacks', *Deutsche Welle*, first published on 06.02.2013, http://www.dw.de/us-considering-pre-emptive-cyberattacks/a-16578359, last assessed on 14.10.2014.

Lee, Dave, 'The daunting challenge of reporting on Cyberwar', *BBC News*, first published on 19.01.2015, http://www.bbc.co.uk/news/technology-30813585, last accessed on 19.01.2015.

Lee, Dave, and Kwek, Nick, 'North Korean hackers 'could kill', warns key defector', *BBC News*, first published on 29.05.2015, http://www.bbc.co.uk/news/technology-32925495, last accessed on 29.05.2015.

Lee, David, 'Facebook's next big thing: Bots for Messenger', *BBC News*, first published on 12.04.2016, http://www.bbc.co.uk/news/technology-36021889, last accessed on 13.04.2016.

Lewis, James, A., 'Liu Jodie 'So What Does the USA Freedom Act Do Anyway?', *Lawfareblog*, first published 03.06.2015, https://www.lawfareblog.com/so-what-does-usa-freedom-act-do-anyway, last accessed 03.06.2015.

Livingstone, David, 'The Intersection of Space and Cyber Security is a Growing Concern', *Chatham House*, first published on 25.11.2014, http://www.chathamhouse.org/expert/comment/16325, last accessed on 27.11.2014.

Lori, Hinnant, and Ken, Dilanian, 'For US Allies, Paradigm Shift In Intelligence Collection', *Associated Press*, first published on 20.05.2015, http://hosted.ap.org/dynamic/stories/E/EU_RETHINKING_INTEL?SITE=AP&SECTION=HOME&TEMPLATE=DEFAULT, last accessed on 21.05.2015.

Macalister, Terry, 'UK energy infrastructure 'at risk of shutdown from cyber-attacks'' *The Guardian*, first published on 18.10.2013 accessed via Nexis Business and News.

MacAskill, Ewen, 'Germany drops inquiry into claims NSA tapped Angela Merkel's phone', *The Guardian*, first published 12.06.2015, accessed via Nexis Business and News.

McCarthy, Tom, 'Syrian Electronic Army takes credit for attack on Obama's Twitter account', *The Guardian*, first published 28.10.2013, http://www.theguardian.com/technology/2013/oct/28/barack-obama-twitter-hacked-syria, last accessed on 18.03.2015.

McConnell, Mike, 'To win the cyber-war, look to the Cold War', *The Washington Post*, first published on 28.02.2010, accessed via Nexis Business and News.

McDonald, Henry, 'Technology: Uphill battle to defend cyberspace: Internet security firm warns of growing threat as attacks by states and criminals rise', *The Guardian*, first published on 06.05.2013, accessed via Nexis Business and News.

McGreal, Chris, 'US set to revive propaganda war as Putin's PR machine 'undermines' Baltic states'', *The Guardian*, first published 25.04.2015, http://www.theguardian.com/world/2015/apr/25/us-set-to-revive-propaganda-war-as-putin-pr-machine-undermines-baltic-states, last accessed on 25.04.2015.

Mendoza, Martha, 'AP IMPACT: US agencies struggle vs. cyberattacks', *The Associated Press*, first published on 11.11.2014, http://m.apnews.com/ap/db_289563/contentdetail.htm?contentguid=0Gbe8xyA, last accessed on 11.11.2014.

Michael, Gallagher, 'Web War II: What a future cyberwar will look like' *BBC News*, first published on 30.04.2012, http://www.bbc.co.uk/news/magazine-17868789, last accessed on 15.10.2014.

Miller, Greg, and Higham, Scott, 'In a propaganda war, U.S. tried to play by the enemy's rules; Confronting The 'Caliphate'', *The Washington Post Blogs*, first published on 08.05.2015, accessed via Nexis Business and News.

Miller, Greg, Nakashima, Ellen, and Tate, Julie, 'CIA Looks to Expand its Cyber Espionage Capabilities', *The Washington Post* first published 23.02.2015, http://www.washingtonpost.com/world/national-security/cia-looks-to-expand-its-cyber-espionage-capabilities/2015/02/23/a028e80c-b94d-11e4-9423-f3d0a1ec335c_story.html?hpid=z3, last accessed on 24.02.2015.

Moskvitch, Katia, 'The world's five biggest cyber threats', *BBC News*, first published on 26.04.2012, http://www.bbc.co.uk/news/technology-17846185, last accessed on 19.03.2015.

Nakashima, Ellen, 'Defense Secretary unveils Pentagon cyberstrategy', *The Washington Post*, first published 22.04.2015, http://www.washingtonpost.com/world/national-security/defense-secretary-unveils-pentagon-cyberstrategy/2015/04/22/959ffcd0-e90a-11e4-aae1-d642717d8afa_story.html, last accessed on 23.04.2015.

Nakashima, Ellen, 'Iran blamed for cyberattacks on U.S. banks and companies' *The Washington Post*, first published on 21.09.2012, http://www.washingtonpost.com/world/national-security/iran-blamed-for-cyberattacks/2012/09/21/afbe2be4-0412-11e2-9b24-ff730c7f6312_story.html, last accessed on 16.02.2015

Nakashima, Ellen, 'New agency to sniff out threats in cyberspace', *The Washington Post* first published on 10.02.2015, http://www.washingtonpost.com/world/national-security/white-house-to-create-national-center-to-counter-cyberspace-intrusions/2015/02/09/a312201e-afd0-11e4-827f-93f454140e2b_story.html, last accessed on 10.02.2015.

Nakashima, Ellen, 'With Plan X, Pentagon seeks to spread U.S. military might to cyberspace', *The Washington Post*, first published on 30.05.2012,

http://www.washingtonpost.com/world/national-security/with-plan-x-pentagon-seeks-to-spread-us-military-might-to-cyberspace/2012/05/30/gJQAEca71U_story.html, last accessed on 28.05.2015.

Nakashima, Ellen, and Whitlock, Craig, 'Hackers breach some White House computers', *The Washington Post*, first published on 28.10.2014, http://www.washingtonpost.com/world/national-security/hackers-breach-some-white-house-computers/2014/10/28/2ddf2fa0-5ef7-11e4-91f7-5d89b5e8c251_story.html, last accessed on 16.02.2015.

Nield, David, 'Finland admits it's suffered a massive cyber-attack. Is the same thing happening across Europe?', *The Daily Telegraph*, first published on 12.11.2013, http://blogs.telegraph.co.uk/technology/davidnield/100011456/finland-admits-its-suffered-a-massive-cyber-attack-is-the-same-thing-happening-across-europe/, last accessed on 14.10.2014.

No author given 'US 'tapped N Korea computers in 2010' report claims', *BBC News*, first published on 19.01.2015, http://www.bbc.co.uk/news/technology-30879637, last accessed on 19.01.2015.

No author given, ''Captured Russian troops 'in Ukraine by accident'', *BBC News*, first published 26.08.2014, http://www.bbc.co.uk/news/world-europe-28934213, last accessed 10.07.2017.

No author given, ''Cyber attack war games' to be staged by UK and US', *BBC News*, first published on 16.01.2015, http://www.bbc.co.uk/news/uk-politics-30842669, last accessed on 16.01.2015.

No author given, 'BBC Monitoring quotes from China, Taiwan press 3 Jun 11' BBC Worldwide Monitoring first published on 03.07.2011

No author given, 'China tightens control on instant messaging services', *BBC News*, first published on 7.08.2014, http://www.bbc.co.uk/news/world-asia-china-28694890, last accessed on 08.10.2014.

No author given, 'Cyber attack takes down Dutch government sites', *BBC News*, first published on 12.02.2015, http://www.bbc.co.uk/news/technology-31440973, last accessed on 12.02.2015.

No author given, 'Cyber-attacks hit British Airways, GitHub and Slack', *BBC News* first published on 30.03.2015, http://www.bbc.co.uk/news/technology-32115292, last accessed on 30.03.2015.

No author given, 'Energy firms hacked by 'cyber-espionage group Dragonfly'', *BBC News*, first published on 1 July 2014, http://www.bbc.co.uk/news/technology-28106478, last accessed 24.11.2014.

No author given, 'GitHub cleans up after cyber-attack', *The Guardian*, first published on 30.03.2015, http://www.theguardian.com/technology/2015/mar/30/github-cleans-up-cyber-attack, last accessed on 30.03.2015.

No author given, 'Latvian paper chides government for lack of cyber security' *BBC Monitoring Europe*, first published on 24.11.2009, accessed from Nexis Business and News.

No author given, 'Microsoft 'deeply sorry' for racist and sexist tweets by AI chatbot' *The Guardian*, first published on 26.03.2016, https://www.theguardian.com/technology/2016/mar/26/microsoft-deeply-sorry-for-offensive-tweets-by-ai-chatbot, last accessed on 06.04.2016.

No author given, 'NATO 'unprepared' for Russia threat, say MPs', *BBC News*, first published on 31.07.2014, http://www.bbc.co.uk/news/uk-politics-28577904, last Accessed on 08.10.2014.

No author given, 'North Korea blames U.S. for Internet shutdown', *CBS News* first published 27.12.2014, http://www.cbsnews.com/news/north-korea-blames-u-s-for-internet-shutdown/,last accessed on 04.02.2015.
No author given, 'North Korea's internet temporarily blacked out', *The Guardian*, first published on 23.12.2014, http://www.theguardian.com/world/2014/dec/22/north-korea-suffers-internet-blackout, last accessed on 04.02.2015.
No author given, 'Security firms uncover 'sophisticated' Regin spyware', *BBC News*, first published on 24.11.2014, http://www.bbc.co.uk/news/technology-30145265, last accessed on 24.11.2014.
No author given, 'South Korea nuclear firm to hold cyber-attack drills after hack', *BBC News*, first published on 22.12.2014, http://www.bbc.co.uk/news/world-asia-30572575, last accessed on 22.12.2014.
No author given, 'South Korea to develop Stuxnet-like cyberweapons', *BBC News*, first published on 21.02. 2014, http://www.bbc.co.uk/news/technology-26287527, last accessed on 24.11.2014.
No author given, 'U.S. may accuse North Korea in Bangladesh cyber heist: WSJ', *Reuters*, first published on 22.03.2017, http://www.reuters.com/article/us-cyber-heist-bangladesh-northkorea-idUSKBN16T2Z3?il%3D0, last accessed on 22.03.2017.
No author given, 'UK to create new cyber defence force', *BBC News*, first published on 29.09.2013, http://www.bbc.co.uk/news/uk-24321717, last accessed on 23.04.2015.
No author given, 'US Centcom Twitter account 'hacked by Islamic State'', *BBC News*, first published on 12.01.2015. http://www.bbc.co.uk/news/world-us-canada-30785232, last accessed 12.01.2015.
No author given, 'US government warns over vulnerable control systems', *BBC News*, first published on 11.01.2013, http://www.bbc.co.uk/news/technology-20984827, last Accessed on 15.10.2014.
Omand, David, 'Understanding digital intelligence from a British perspective', *STRIFE*, first published on 05.02.2015, http://strifeblog.org/2015/02/05/understanding-digital-intelligence-from-a-british-perspective/, last accessed on 06.02.2015.
Park, Ju-Min, and Cho, Meeyoung, 'South Korea blames North Korea for December hack on nuclear operator', *Reuters*, first published on 17.03.2015, http://uk.reuters.com/article/2015/03/17/uk-nuclear-southkorea-northkorea-idUKKBN0MD1F420150317, last accessed on 18.03.2015.
Park, Ju-Min, and Pearson, James, 'North Korea's cyber spies exposed: Inside the secretive cyber-warfare cell Bureau 121', *The Independent*, first published on 05.12.2014, http://www.independent.co.uk/news/world/asia/north-koreas-cyber-spies-exposed-inside-the-secretive-cyberwarfare-cell-bureau-121-9907161.html, last accessed on 05.12.2014.
Peachey, Paul, 'Cyber crime: First online murder will happen by end of year, warns US firm', *The Independent*, first published 05.10.2014, http://www.independent.co.uk/life-style/gadgets-and-tech/news/first-online-murder-will-happen-by-end-of-year-warns-us-firm-9774955.html, last accessed on 08.10.2014.
Perlroth, Nicole, 'At RSA Conference, Computer Security Done Right and Wrong' *The New York Times*, first published on 22.04.2015, http://bits.blogs.nytimes.com/2015/04/22/at-rsa-conference-computer-

security-done-right-and-wrong/?mabReward=A2&action=click&pgtype=Homepage&region=CColumn&module=Recommendation&src=rechp&WT.nav=RecEngine, last accessed on 23.04.2015.

Perlroth, Nicole, and Sanger, David, E., 'U.S. Embedded Spyware, Report Says', *The New York Times*, first published on 17.02.2015, accessed via Nexis Business and News.

Piper, Elizabeth, 'Putin says Western spies plot against Russia before polls', *Reuters* first published on 26.03.2015, http://uk.reuters.com/article/2015/03/26/uk-russia-crisis-putin-idUKKBN0MM1RZ20150326, last accessed on 26.03.2015.

Riley, Michael, A., and Robertson, Jordan, 'Security Firms Tie Russian Government to Utilities Hacks', *Bloomberg*, first published on 30.10.2014, http://www.bloomberg.com/politics/articles/2014-10-30/security-firms-tie-russian-government-to-utilities-hacks, last accessed on 25.11.2014.

Robertson, Jordan, 'Security Companies Hire Hackers, Ex-Spies to Fight Cyber Attacks', *Bloomberg*, first published on 14.04.2015, http://www.bloomberg.com/news/articles/2015-04-14/security-companies-hire-hackers-ex-spies-to-fight-cyber-attacks, last accessed on 15.04.2015.

Rogers, Mike, 'Mike Rogers: U.S. businesses are in an unfair fight against cyberthreats', *The Washington Post*, first published on 23.10.2013, http://www.washingtonpost.com/opinions/mike-rogers-us-businesses-are-in-an-unfair-fight-against-cyberthreats/2013/10/22/5a5167b8-3b32-11e3-b6a9-da62c264f40e_story.html, last accessed on 17.02.2015.

Rushe, Dominic, 'JP Morgan Chase reveals massive data breach affecting 76m households', *The Guardian*, first published 03.10.2014, https://www.theguardian.com/business/2014/oct/02/jp-morgan-76m-households-affected-data-breach, last accessed 03.10.2014.

Sanger, David, E., 'Countering Cyberattacks Without a Playbook', *The New York Times*, first published on 24.12.2014, accessed via Nexis Business and News.

Sanger, David, E., 'Document Reveals Growth of Cyberwarfare Between the U.S. and Iran' *The New York Times*, first published on 23.02.2015, accessed via Nexis Business and News.

Sanger, David, E., 'N.S.A. chief says that damage from Snowden leaks is manageable', *The New York Times*, first published on 01.07.2014, accessed via Nexis Business and News.

Sanger, David, E., 'NATO set to ratify cyberattack pledge; Strike on any member could be treated as if it were against them all', *The New York Times*, first published on 02.09.2014, accessed via Nexis Business and News.

Sanger, David, E., 'Obama lets N.S.A. exploit online security flaws, officials say', *The New York Times*, first published on 14.04.2014, accessed via Nexis Business and News.

Sanger, David, E., 'Obama Order Sped Up Wave of Cyberattacks Against Iran', *The New York Times*, first published on 01.06.2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=2&_r=3&seid=auto&smid=tw-nytimespolitics&pagewanted=all&, last accessed on 09.10.2014.

Sanger, David, E., 'U.S. Must Step Up Capacity for Cyberattacks, Chief Argues' *The New York Times*, first published on 20.03.2015, accessed via Nexis Business and News.

Sanger, David, E., 'U.S. offers assurances to China on cyberattacks; Visit by Pentagon chief was preceded by briefing for Beijing's top officers', *The New York Times*, first published on 08.04.2014, accessed via Nexis Business and News.

Sanger, David, E., 'U.S. reaches out to China on cyberwar; Officers from Beijing get briefing in effort to avoid future escalations', *The New York Times*, first published on 07.04.2014, accessed via Nexis Business and News.

Sanger, David, E., and Broad, William, J., 'Unstated Factor in Iran Talks: Threat of Nuclear Tampering', *The New York Times*, 21.03.2015 http://www.nytimes.com/2015/03/22/world/middleeast/unstated-factor-in-iran-talks-threat-of-nuclear-tampering.html?_r=0, last accessed on 24.03.2015,

Sanger, David, E., and Perlroth, Nicole, 'Iran Is Raising Sophistication and Frequency of Cyberattacks, Study Says', *The New York Times*, first published on 15.04.2015, http://www.nytimes.com/2015/04/16/world/middleeast/iran-is-raising-sophistication-and-frequency-of-cyberattacks-study-says.html?_r=2#story-continues-3, last accessed on 20.04.2015.

Sanger, David, E., and Perlroth, Nicole, 'Obama Heads to Security Talks Amid Tensions', *The New York Times*, first published on 12.02.2015, http://www.nytimes.com/2015/02/13/business/obama-heads-to-security-talks-amid-tensions.html?hp&action=click&pgtype=Homepage&module=first-column-region&region=top-news&WT.nav=top-news&_r=0, last accessed on 13.02.2015.

Sanger, David, E., and Perlroth, Nicole, 'Russians' testing of West revives Cold War custom', *The New York Times*, first published on 01.11.2014, accessed via Nexis Business and News.

Sanger, David, E., and Perlroth, Nicole, 'U.S. hacked Chinese servers it saw as spy risk; N.S.A. took information on telecom giant and looked for ties to military', *The New York Times*, first published on 24.03.2014, accessed via Nexis Business and News.

Sanger, David, E., and Schmitt, Eric, 'Hackers Use Old Lure on Web to Help Syrian Government', *The New York Times*, first published on 01.02.2015, http://www.nytimes.com/2015/02/02/world/middleeast/hackers-use-old-web-lure-to-aid-assad.html?smid=nytcore-ipad-share&smprod=nytcore-ipad&_r=0, last accessed on 02.02.2015.

Savage, Charlie, Angwin, Julia, Larson, Jeff, and Moltke, Henrik, 'Hunting for Hackers, N.S.A. Secretly Expands Internet Spying at U.S. Border', *The New York Times*, first published on 04.06.2015, http://www.nytimes.com/2015/06/05/us/hunting-for-hackers-nsa-secretly-expands-internet-spying-at-us-border.html, last accessed on 09.06.2015.

Schmitt, Eric, 'U.S. Intensifies Effort to Blunt ISIS' Message', *The New York Times*, first published on 16.02.2015, http://www.nytimes.com/2015/02/17/world/middleeast/us-intensifies-effort-to-blunt-isis-message.html?hp&action=click&pgtype=Homepage&module=first-column-region&region=top-news&WT.nav=top-news, last accessed on 17.02.2015.

Sean, Farrel, 'TalkTalk counts costs of cyber-attack', *The Guardian*, first published on 02.12.2016, http://www.theguardian.com/business/2016/feb/02/talktalk-cyberattack-costs-customers-leave, last accessed on 03.02.2016.

Sengupta, Kim, 'Ukraine: Where a dark world of hybrid warfare and murky loyalties prevails', *The Independent*, first published on 23.02.2015,

http://www.independent.co.uk/news/world/europe/in-ukraine-a-dark-world-of-hybrid-warfare-and-murky-loyalties-prevails-10066132.html, last accessed on 24.02.2015.

Shachtman, Noah, 'Iran Now a 'Top Threat' to U.S. Networks, Spy Chief Claims', *Wired*, first published on 31.01.2012, http://www.wired.com/2012/01/iran-now-a-top-threat-to-u-s-networks-spy-chief-says/, last accessed on 17.02.2015.

Shen, Lucinda, '7 things we learned about the frat brothers linked to JPMorgan Hack', *Business Insider UK*, first published 06.08.2015, http://uk.businessinsider.com/7-things-we-learned-about-the-frat-brothers-linked-to-jp-morgan-hack-2015-8?r=US&IR=T, last accessed on 06.08.2015.

Smith, David, and Roberts, Dan, 'CIA Chief Criticises recent Surveillance Rollbacks in wake of Paris Attacks', *The Guardian*, first published 16.11.2015, https://www.theguardian.com/world/2015/nov/16/cia-director-john-brennan-criticises-surveillance-reform-paris-attacks, last accessed on 16.11.2015.

Smith, David, Jacobs, Ben, Swaine, Jon, and Walker, Shaun, 'Trump Jr was told of Russian efforts to help campaign – report', *The Guardian*, first published on 11.07.2017, https://www.theguardian.com/us-news/2017/jul/10/donald-trump-jr-russia-meeting-clinton-statements, last accessed on 11.07.2017.

Snyder, Charley, and Sulmeyer, Michael, 'Decoding the 2017 NDAA's Provisions on DoD Cyber Operations', *Lawfareblog*, first published 30.01.2017, https://www.lawfareblog.com/decoding-2017-ndaas-provisions-dod-cyber-operations, last accessed on 10.07.2017.

Spillius, Alex, 'US at risk of 'cyber-Pearl Harbor', Leon Panetta warns' *The Daily Telegraph* first published 12.10.2012, http://www.telegraph.co.uk/news/worldnews/northamerica/usa/9604794/US-at-risk-of-cyber-Pearl-Harbor-Leon-Panetta-warns.html, last accessed on 04.02.2015.

Sternstein, Aliya, 'The Military's Cybersecurity Budget in 4 Charts', *Defense One*, first published on 16.03.2015, http://www.defenseone.com/management/2015/03/militarys-cybersecurity-budget-4-charts/107679/, last accessed on 18.03.2015.

Strohm, Chris, 'North Korea Web Outage Response to Sony Hack, Lawmaker Says', *Bloomberg*, first published on 17.03.2015, http://www.bloomberg.com/politics/articles/2015-03-17/north-korea-web-outage-was-response-to-sony-hack-lawmaker-says, last accessed on 19.03.2015.

Syrian Electronic Army, 'Twitter Feed', https://twitter.com/Official_SEA16/media, published 01.02.2014.

The Rachel Maddow Show, 'Maddow to news orgs: beware of forged Trump Russia documents!', first published 06.07.2017, http://www.msnbc.com/rachel-maddow/watch/maddow-to-news-orgs-heads-up-for-hoaxes-985491523709, last accessed on 06.07.2017.

Traynor, Ian, 'Russia accused of unleashing cyberwar to disable Estonia', *The Guardian*, first published 17.05.2007, http://www.theguardian.com/world/2007/may/17/topstories3.russia, last accessed on 13.02.2015.

US Government, Department of Defense, 'Cybercom Chief Details Strategic Priorities for 2016', http://www.defense.gov/News-Article-

View/Article/643954/cybercom-chief-details-strategic-priorities-for-2016, last accessed on 25.01.2016.

US Government, Department of State, 'Welcome to the "Islamic State" land', https://www.youtube.com/watch?v=-wmdEFvsY0E&oref=https%3A%2F%2Fwww.youtube.com%2Fwatch%3Fv%3D-wmdEFvsY0E&has_verified=1, last accessed on 08.03.2016.

Usborne, David, 'US Central Command 'hacked' by Islamic State supporters', *The Independent*, first published on 12.01.2015, http://www.independent.co.uk/news/world/americas/us-central-command-hacked-by-islamic-state-supporters-9973615.html, last accessed on 12.01.2015.

Vincent, James, 'GCHQ's spy toolkit: Leaked documents reveal how UK manipulates information online The Independent webpage', *The Independent*, first published on 14.07.2014, http://www.independent.co.uk/life-style/gadgets-and-tech/gchqs-spy-toolkit-leaked-documents-reveal-how-uk-manipulates-information-online-9606043.html, last accessed 08.10.2014.

Vincent, James, 'Russian nuclear power plant infected by Stuxnet malware says cyber-security expert', *The Independent*, first published on 12.11.2013, http://www.independent.co.uk/life-style/gadgets-and-tech/news/russian-nuclear-power-plant-infected-by-stuxnet-malware-says-cybersecurity-expert-8935529.html, last accessed on 09.10.2014.

Vistica, Gregory, L., 'Cyberwar and Sabotage', *Newsweek Atlantic Edition*, first published on 31.05.1999, accessed via Nexis Business and News.

Ward, Mark, 'How to hack a nation's infrastructure', *BBC News*, first published on 20.05.2013, http://www.bbc.co.uk/news/technology-22524274, last accessed on 15.10.2014.

Ward, Mark, 'Microsoft patches bug 'used by Chinese hackers'', *BBC News*, first published on 10.02.2015, http://www.bbc.co.uk/news/technology-31381892, last accessed 10.02.2015.

Westcott, Richard, 'Rail signal upgrade 'could be hacked to cause crashes'', *BBC News*, first published on 24.04.2015, http://www.bbc.co.uk/news/technology-32402481, last accessed on 24.04.2015.

Williams-Grut, Oscar, 'Caught in the crossfire of a cyber Cold War; Fears are mounting that Vladimir Putin has instructed hackers to target banks like JP Morgan', *The Independent* first published on 29.08.2014, accessed from Nexis Business and News.

Withnall, Adam, 'The Interview hacking: Sony accused of 'collapse in America's first cyberwar' after cancelling release of Kim Jong-un assassination film', *The Independent*, first published on 18.12.2014, http://www.independent.co.uk/news/world/americas/the-interview-hacking-sony-accused-of-collapse-in-americas-first-cyberwar-after-cancelling-release-of-kim-jongun-assassination-film-9932628.html, last accessed on 18.12.2014.

Wong, Edward, 'American firms in China feel the heat of cyberdispute', *The New York Times*, first published on 02.06.2014, accessed via Nexis Business and News.

Zetter, Kim, 'An Unprecedented Look at Stuxnet, the World's First Digital Weapon', *Wired*, first published on 03.11.14, http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/, last accessed on 05.11.2014.

Zetter, Kim, 'Report: Stuxnet Hit 5 Gateway Targets On Its Way To Iranian Plant' *Wired*, first published, 11.02.2011, http://www.wired.com/2011/02/stuxnet-five-main-target/, last accessed on 03.03.2015.

Zetter, Kim, 'Simulated Cyberattack Shows Hackers Blasting Away At The Power Grid', *Wired*, first published on 09.26.07, http://www.wired.com/2007/09/simulated-cyber/, last accessed on 03.03.2015.

Secondary Works: Articles and Papers

Abu, Ali, Amer, Nizar and Sisan, Saeb, 'A Corporation Cyber War Strategy', *GSTF Journal on Computing* (JoC), 3:3, (2014), 12-20.

Aistrope, Tim, 'Social Media and Counterterrorism Strategy', *Australian Journal of International Affairs*, 70:2, (2016), 121-138.

Aldrich, Richard J., ''Grow Your Own': Cold War Intelligence and History Supermarkets', Intelligence and National Security, 17:1, (2002), 135-152.

Amble, John Curtis, 'Combating Terrorism in the New Media Environment', *Studies in Conflict & Terrorism*, 35:5, (2012), 339-353.

Andregg, Michael, 'Ethics and Professional Intelligence', in Loch K. Johnson (ed), *The Oxford Handbook of National Security Intelligence*, (Oxford: Oxford University Press, 2010).

Andrew, Christopher, 'Intelligence, International Relations and 'Under-theorisation'', *Intelligence and National Security*, 19:2, (2004), 170-184.

Angstrom, Jan, 'Introduction: Debating the Nature of War' in Isabelle Duyvesteyn and Jan Angstrom (eds) Rethinking the Nature of War (London: Frank Cass, 2005)

Arquilla, John, 'Ethics and Information Warfare', in: Z. Khalizad, J. White & A. Marshall (Eds), Strategic Appraisal: The Changing Role of Information in Warfare, (Santa Monica, CA: RAND Corporation, 2000).

Arquilla, John, 'Twenty Years Of Cyberwar', *Journal of Military Ethics*, 12:1, (2013), 80-87.

Arquilla, John, and Ronfeldt, David, 'Cyberwar is coming!', *Comparative Strategy*, 12:2, (1993), 141-165.

Arquilla, John, and Ronfeldt, David, 'The Advent of Netwar (revisited)', in John Arquilla and David Ronfeldt (eds), *Networks and Netwars: The Future of Terror, Crime, and Militancy*, (Arlington: RAND, 2001).

Baker, James E., 'Covert Action: United States Laws in Substance, Process, and Practice' in Loch K. Johnson (ed) *The Oxford Handbook of National Security and Intelligence*, (Oxford: Oxford University Press, 2010).

Barrett, Edward T., 'Warfare in a New Domain: The Ethics Of Military Cyber-Operations', *Journal of Military Ethics*, 12:1, (2013), 4-17.

Barry, James, 'Managing Covert Political Action', in Jan Goldman (ed), *Ethics of Spying: A Reader for the Intelligence Professional* (Lanham: Scarecrow Press, 2006).

Barzashka, Ivanka, 'Are Cyber-Weapons Effective?', *The RUSI Journal*, 158:2, (2013), 48-56.

Beard, Mathew, 'Just War, Cyberwar, and Cyber Espionage', in Jai Galliott and Warren Reed (eds), *Ethics and the Future of Spying: Technology, National Security, and Intelligence Collection* (London: Routledge, 2016).

Beitz, Charles R., 'Covert Intervention as a Moral Problem', in Jan Goldman (ed) *The Ethics of Spying: A Reader for Intelligence Professionals* (Maryland: Scarecrow Press, 2006).

Bellaby, Ross W., 'Justifying Cyber-intelligence?', *Journal of Military Ethics*, 15:4, (2016), 299-319.

Betz, David, 'Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed', *Journal of Strategic Studies*, 35:5, (2012), 689-711.

Beyerchen, Alan, 'Clausewitz, Nonlinearity, and the Unpredictability of War', *International Security*, 17:3, (1992), 59-90

Black, Jeremy, 'What is War'?, *The RUSI Journal*, 152:6, (2007), 42-45.

Bluth, Christoph, 'The British Resort to Force in the Falklands/Malvinas Conflict 1982: International Law and Just War Theory', *Journal of Peace Research*, 24:1, (1987), 5-20.

Brantly, Aaron F., 'Cyber Actions by State Actors: Motivation and Utility', *International Journal of Intelligence and CounterIntelligence*, 27:3, (2014), 465-484.

Brodie, Bernard, 'A Guide to the Reading of On War' in Carl von Clausewitz *On War*, Michael Howard and Peter Paret edited and translated, (Princeton: Princeton University Press, 1976).

Brown, Davis, 'Judging The Judges: Evaluating Challenges To Proper Authority In Just War Theory', *Journal of Military Ethics*, 10:3, (2011), 133-147.

Brown, Gary D., 'Proportionality and Just War', *Journal of Military Ethics*, 2:3, (2003), 171-185.

Cavelty, Myriam Dunn, 'Cyberwar' George Kassimeris and John Buckley (eds) *The Ashgate Research Companion to Modern Warfare* (Surrey: Ashgate Publication, 2010).

Chin, Warren, 'Examining the Application of British Counterinsurgency Doctrine by the American Army in Iraq', *Small Wars & Insurgencies*, 18:1, (2007), 1-26

Codevilla, Angelo, and Gobson, Roy, 'Intelligence (Covert action and counterintelligence) as an Instrument of Policy' in Roy Gobson (ed) *Intelligence Requirements for the 1980's: Intelligence and Policy* (Washington DC: Lexington Books, 1986).

Colby, William E., 'Public Policy, Secret Action', *Ethics and International Affairs*, 3:1, (1989), 61-71.

Cole, Darrell, 'War and Intention', *Journal of Military Ethics*, 10:3, (2011), 174-191.

Cook, Colonel James, ''Cyberation' and Just War Doctrine: A Response to Randall Dipert', *Journal of Military Ethics*, 9:4, (2010), 411-423.

Cormac, Rory, Goodman, Michael S., and Holman, Tom, 'A Modern Day Requirement for Co-Ordinated Covert Action', *The RUSI Journal*, 161:2, (2016), 14-21.

Daugherty, William J. 'The Role of Covert Action' in Loch K. Johnson (ed), *Handbook of Intelligence Studies* (London: Routledge, 2007).

Daugherty, William J., 'Approval and Review of Covert Action Programs Since Reagan', *International Journal of Intelligence and CounterIntelligence*, 17:1, (2004), 62-80.

Daugherty, William J., 'Covert Action: Strengths and Weaknesses' in Loch K. Johnson (ed), *The Oxford Handbook of National Security and Intelligence* (Oxford: Oxford University Press, 2010).

Davies, Philip H.J., 'Intelligence and the Machinery of Government Conceptualizing the Intelligence Community' *Public Policy and Administration*, 25:1, (2010), 29-46.
Davies, Philip H.J., 'Spies as Informants: Triangulation and the Interpretation of Elite Interview Data in the Study of the Intelligence and Security Services', *Politics*, 21:1, (2001), 73-80.
Deakin, Stephen, 'Wise Men And Shepherds: A Case For Taking Non-Lethal Action Against Civilians Who Discover Hiding Soldiers', *Journal of Military Ethics*, 10:2, (2011), 110-119.
Dipert Randall R., 'Preventive War and the Epistemological Dimension of the Morality of War', *Journal of Military Ethics*, 5:1, (2006), 32-54.
Dipert, Randall R., 'The Ethics of Cyberwarfare', *Journal of Military Ethics*, 9:4, (2010), 384-410.
Dylan Huw, 'Super-Weapons and Subversion: British Deterrence by Deception Operations in the Early Cold War', *Journal of Strategic Studies*, 38:5, (2015), 704-728.
Eberle, Christopher J., 'Just War And Cyberwar', *Journal of Military Ethics*, 12:1, (2013), 54-67.
Echevarria, Antulio J. II, 'Strategic Thought: The Relevance of Clausewitz' in John Buckley and George Kassimeris (eds) *The Ashgate Research Companion to Modern Warfare* (Surrey: Ashgate Publishing Limited, 2010).
Eckstein, Harry, 'Case Study and Theory in Political Science', in Roger Gomm, Martyn Hammersley, and Peter Foster (eds), *Case Study Method: Key Issues, Key Texts*, (London: SAGE Publications, 2000).
Eisenhardt, Kathleen M., 'Building Theories from Case Study Research', *The Academy of Management Review*, 14:4, (1989), 532-550.
Erskine, Toni, "As Rays of Light to the Human Soul'? Moral Agents and Intelligence Gathering', *Intelligence and National Security*, 19:2, (2004), 359-381.
Etges, Andreas, 'All that Glitters is Not Gold: The 1953 Coup against Mohammed Mossadegh in Iran', *Intelligence and National Security*, 26:4, (2011), 495-508.
Farwell, James P., and Rohozinski, Rafal, 'Stuxnet and the Future of Cyber War', *Survival*, 53:1, (2011), 23-40
Fleming, Colin M., 'New or Old Wars? Debating a Clausewitzian Future', *Journal of Strategic Studies*, 32:2, (2009), 213-241.
Freedman, Lawrence, 'General Introduction' in Lawrence Freedman (ed) *War* (Oxford: Oxford University Press, 1994).
Galeotti, Mark, 'Hybrid, Ambiguous, and Non-linear? How New is Russia's 'New Way of War'?', *Small Wars & Insurgencies*, 27:2, (2016), 282-301.
Gallo, André Le, 'Covert Action: A Vital Option in U.S. National Security Policy', *International Journal of Intelligence and CounterIntelligence*, 18:2, (2005), 354-359, 356-357.
Gartzke, Erik, and Lindsay, Jon R., 'Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace', *Security Studies*, 24:2, (2015), 316-348.
Gendron, Angela, 'Just War, Just Intelligence: An Ethical Framework for Foreign Espionage', *International Journal of Intelligence and CounterIntelligence*, 18:3, (2005), 398-434.
Gill, Peter, 'Evaluating Intelligence Oversight Committees: The UK Intelligence and Security Committee and the 'war on terror'', *Intelligence and National Security*, 22:1, (2007), 14-37.

Glenny, Misha and Kavanagh, Camino, '800 Titles but No Policy—Thoughts on Cyber Warfare, American Foreign Policy Interests' *The Journal of the National Committee on American Foreign Policy*, 34:6, (2012), 287-294.
Goodman, Melvin A., 'Espionage and Covert Action', in Craig Eisendrath (ed), *National Insecurity: U.S. Intelligence After the Cold War* (Philadelphia: Temple University Press, 2000).
Grobler, Marthie, and Vuuren, Joey Jansen van, 'Collaboration as proactive measure against cyber warfare in South Africa', *African Security Review*, 21:2, (2012), 61-73.
Hellman, Maria and Wagnsson, Charlotte, 'How can European states respond to Russian Information Warfare? An analytical framework', *European Security*, 26:2, (2017), 153-170.
Herman, Michael, 'Ethics and Intelligence after September 2001', *Intelligence and National Security*, 19:2, (2004), 342-358.
Herman, Michael, 'Modern Intelligence Services: Have They a Place in Ethical Foreign Policy', in Harold Shukman (ed), *Agents for Change: Intelligence Services in the 21st Century*, (London: St Ermin's Press, 2000).
Hillebrand, Claudia, 'The Role of News Media in Intelligence Oversight', *Intelligence and National Security*, 27:5, (2012), 689-706.
Hollis, David, 'Cyberwar Case Study: Georgia 2008', *Small Wars Journal*, http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008, last accessed on 12.02.2015.
Howard, Michael, 'Jomini and the Classical Tradition in Military Thought', in Michael Howard (ed) *The Theory and Practice of War* (Indiana: Indiana University Press, 1975).
Jajko, Walter, 'Deception: Appeal for Acceptance; Discourse on Doctrine; Preface to Planning', *Comparative Strategy*, 21:5, 2002, 351-363.
Jean-Loup, Samaan, 'Cyber Command', *The RUSI Journal*, 155:6, (2010), 16-21.
Jeffrey, T. Richelson, 'When Kindness Fails: Assassination as a National Security Option', *International Journal of Intelligence and CounterIntelligence*, 15:2, (2002), 243-274.
Johnson, Loch K., 'A Shock Theory of Congressional Accountability for Intelligence', in Loch K. Johnson (ed), *The Handbook of Intelligence Studies* (London: Routledge, 2007).
Johnson, Loch K., 'Ethical Intelligence: A Contradiction in Terms?', in 'A Symposium on Intelligence Ethics', *Intelligence and National Security*, 24:3, (2009), 366-386.
Johnson, Loch K., 'On Drawing a Bright Line for Covert Operations' *American Journal of International Law*, 86.2 (1992), 284-309.
Jonsson, Oscar, and Seely, Robert, 'Russian Full-Spectrum Conflict: An Appraisal After Ukraine', *The Journal of Slavic Military Studies*, 28:1, (2015), 1-22.
Junio, Timothy J., 'How Probable is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate', *Journal of Strategic Studies*, 36:1, (2013), 125-133.
Kaldor, Mary, 'Elaborating the 'New War' Thesis', in Isabelle Duyvesteyn and Jan Angstrom (eds), *Rethinking the Nature of War* (London: Frank Cass, 2005).
Kasher, Asa, 'The Principle of Distinction', *Journal of Military Ethics*, 6:2, (2007), 152-167.
Keen, David, 'Introduction', *The Adelphi Papers*, 38:320, (1998), 9-13.
Kibbe, Jennifer D., 'Covert action and the Pentagon', *Intelligence and National Security*, 22:1, (2007), 57-74.

Kibbe, Jennifer D., 'Covert Action, Pentagon Style' in Loch K. Johnson (ed) *The Oxford Handbook of National Security and Intelligence* (Oxford: Oxford University Press, 2010).
Kibbe, Jennifer D., 'The Rise of the Shadow Warriors', *Foreign Affairs*, 83:2, (2004), 102-115.
King, Ross D., 'Intercept: The Secret History of Computers and Spies', *Intelligence and National Security*, 32:6, (2017), 875-878.
Klimburg, Alexander, 'Mobilising Cyber Power', *Survival: Global Politics and Strategy*, 53:1, (2011), 41-60.
Koblentz, Gregory D., and Brian Mazanec M., 'Viral Warfare: The Security Implications of Cyber and Biological Weapons', *Comparative Strategy*, 32:5, (2013), 418-434.
Kuehl, Dan, 'Introduction: "Brother, Can you Spare Me a DIME"' in Leigh Armistead (ed), *Information Warfare: Separating Hype from Reality*, (Washington DC: Potomac Books, 2007).
Levy, Jack S., 'Case Studies: Types, Designs, and Logics of Inference', *Conflict Management and Peace Science*, 25:1, (2008), 1-18.
Lewis, James A., 'Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats' *Center for Strategic and International Studies*, December 2002.
Liang, Gaoqi, Weller, Steven R., Zhao, Junhua, Luo, Fengji, Dong, Zhao Yang, 'The 2015 Ukraine Blackout: Implications for False Data Injection Attacks' *IEEE Transactions on Power Systems*, 32:4, (2017), 3317-3318.
Liff, Adam P., 'Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War', *Journal of Strategic Studies*, 35:3, (2012), 401-428
Lindsay, Jon R., 'Stuxnet and the Limits of Cyber Warfare', *Security Studies*, 22:3, (2013), 365-404.
McCarthy, Gregory C., 'GOP Oversight of Intelligence in the Clinton Era', *International Journal of Intelligence and CounterIntelligence*, 15:1, (2002), 26-51.
McGraw, Gary, 'Cyber War is Inevitable (Unless We Build Security In)', *Journal of Strategic Studies*, 36:1, (2013), 109-119.
McMahan, Jeff, 'Just Cause for War', *Ethics and International Affairs*, 19:3, (2005), 1-21.
Moran, Christopher, 'Intelligence and the Media: The Press, Government Secrecy and the 'Buster' Crabb Affair', *Intelligence and National Security*, 26:5, (2011), 676-700.
Murphy, Christopher J., and Lomas, Daniel W. B., 'Return to Neverland? Freedom of Information and the History of British Intelligence'. *The Historical Journal*, 57:1, (2014), 273-287.
Murphy, Sean D., 'Terrorism and the Concept of 'Armed Attack' in Article 51 of the U.N. Charter' *Harvard International Law Journal*, 43:1, (2002), 41-51.
O'Brien, Kevin, 'Information Age, Terrorism and Warfare', *Small Wars & Insurgencies*, 14:1, (2003), 183-206.
O'Driscoll, Cian, 'Learning the Language of Just War Theory: The Value of Engagement', *Journal of Military Ethics*, 6:2, (2007), 107-116.
Omand Sir David and Phythian Mark, 'Ethics and Intelligence: A Debate', *International Journal of Intelligence and CounterIntelligence*, 26:1, (2013), 38-63.

Orlov, Alexander, 'The Theory And Practice Of Soviet Intelligence' *Studies in Intelligence* 7:2, (1963), 45-65, https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol7no2/html/v07i2a05p_0001.htm
Ott, Marvin C., 'Partisanship and the Decline of Intelligence Oversight', *International Journal of Intelligence and CounterIntelligence*, 16:1, (2003), 69-94.
Paquette, Laure, 'Strategy and Time in Clausewitz's On War and in Sun Tzu's The Art of War', Comparative Strategy, 10:1, (1991), 37-51.
Paret, Peter, 'Clausewitz' in Peter Paret (ed), *Makers of Modern Strategy: From Machiavelli to the Nuclear Age* (Princeton: Princeton University, 1986).
Paret, Peter, 'Clausewitz and the Nineteenth Century', in Michael Howard (ed) *The Theory and Practice of War* (Indiana: Indiana University Press, 1975).
Paret, Peter, 'The Genesis of On War' in Carl von Clausewitz, *On War*, Michael Howard and Peter Paret edited and translated (Princeton: Princeton University Press, 1976).
Patterson, Eric, and Casale, Teresa, 'Targeting Terror: The Ethical and Practical Implications of Targeted Killing', *International Journal of Intelligence and CounterIntelligence*, 18:4, (2005), 638-652.
Perry, David L., '"Repugnant Philosophy": Ethics, Espionage, and Covert Action', in Jan Goldman (ed), *Ethics of Spying: A Reader for the Intelligence Professional* (Lanham: Scarecrow Press, 2006).
Philp, Mark, 'Political Theory and History', in Marc Stears and David Leopold (eds), *Political Theory: Methods and Approaches* (Oxford: Oxford University Press, 2008).
Pincher, Chapman, 'A Lifetime of Reporting on Intelligence Affairs' in Robert Dover and Robert Goodman (eds) *Spinning Intelligence: Why Intelligence Needs the Media, Why the Media Needs Intelligence* (London: Hurst and Company, 2009).
Prados, John, 'The future of Covert Action' in Loch K. Johnson (ed), *Handbook of Intelligence Studies* (London: Routledge, 2007).
Prillaman, William C., and Dempsey, Michael P., 'Mything the Point: What's Wrong with the Conventional Wisdom about the C.I.A', *Intelligence and National Security*, 19:1, (2004), 1-28.
Pritchard, James, and Smith, M.L.R., 'Thompson in Helmand: Comparing Theory to Practice in British Counter-insurgency Operations in Afghanistan', *Civil Wars*, 12:1-2, (2010), 65-90.
Quinlan, Michael, 'Just intelligence: Prolegomena to an Ethical Theory', *Intelligence and National Security*, 22:1, (2007), 1-13.
Renz, Bettina, 'Russia and 'hybrid warfare'', *Contemporary Politics*, 22:3, (2016) 283-300.
Rid, Thomas, 'Cyber War Will Not Take Place', *Journal of Strategic Studies*, 35:1 (2013), 5-32.
Rid, Thomas, and Buchanan, Ben, 'Attributing Cyber Attacks', *Journal of Strategic Studies*, 38:1-2, (2015), 4-37.
Rosenfield, Daniel K., 'Rethinking Cyber War', *Critical Review: A Journal of Politics and Society*, 21:1, (2009), 77-90.
Sewell, Bevan, 'The Pragmatic Face of the Covert Idealist: The Role of Allen Dulles in US Policy Discussions on Latin America, 1953–61', *Intelligence and National Security*, 26:2-3, (2011), 269-290.
Sharma, Amit, 'Cyber Wars: A Paradigm Shift from Means to Ends', Strategic Analysis, 34:1, (2010), 62-73.

Sharp, Travis, 'Theorizing Cyber Coercion: The 2014 North Korean Operation Against Sony', *Journal of Strategic Studies*, 40:7, (2017), 898-926.
Singer P. W., 'Stuxnet and its Hidden Lessons on the Ethics of Cyber Weapons', *Case Westren Reserve of International Law*, 47:3, (2015), 79-86.
Smith, M.L.R. 'Strategy in an Age of Low-Intensity Warfare: Why Clausewitz is Still more Relevant than His Critics' in Isabelle Duyvesteyn and Jan Angstrom (eds), *Rethinking the Nature of War*, (London: Frank Cass, 2005).
Stempel, John D., 'Covert Action and Diplomacy', *International Journal of Intelligence and CounterIntelligence*, 20:1, (2007), 122-135.
Stone, John, 'Cyber War Will Take Place!', *Journal of Strategic Studies*, 36:1, (2013), 101-108.
Tabansky, Lior, 'Basic Concepts in Cyber Warfare' *Military and Strategic Affairs*, 3:1, (2011), 75-92.
Taylor, Stan A., and Snow, Daniel, 'Cold War Spies: Why They Spied and how They got Caught', *Intelligence and National Security*, 12:2, (1997), 101-125.
Tesón Fernando R., 'Eight Principles for Humanitarian Intervention', *Journal of Military Ethics*, 5:2, (2006), 93-113
Trendle Giles 'Cyberwars: The Coming of the E-Jihad' The Middle East 03050734, Apr2002, Issue 322
Twigge, S., and Scott, L., 'Strategic Defence by Deception', *Intelligence and National Security*, 16:2, (2001) 152-157.
Warner, Michael, 'Wanted A definition of Intelligence', *Studies in Intelligence*, 46:6, 2002, accessed via https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol46no3/article02.html last accessed on 17.10.2016
Waxman, Matthew C., 'Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)' *The Yale Journal Of International Law*, 36:421, (2011), 421-459/
Wirtz, James J., 'The Cyber Pearl Harbor', *Intelligence and National Security*, 32:6, (2017), 758-767.
Wright, Quincy, 'When does War Exist?', *The American Journal of International Law*, 26:2, (1932), 362-368.

Secondary Works: Books and Theses

Aldrich, Richard J., and Cormac, Rory, *The Black Door: Spies, Secret Intelligence and British Prime Ministers* (London: William Collins, 2016).
Aldrich, Richard J., *GCHQ: The Uncensored Story of Britain's Most Secret Intelligence Agency* (London: Harper Press, 2011).
Aldrich, Richard J., *The Hidden Hand: Britain, American and Cold War Secret Intelligence* (London: John Murray, 2001).
Andress, Jason, and Winterfeld, Steve, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*, Second Edition (Waltham: Elsevier, 2014).
Andrew, Christopher, and Gordievsky, Oleg, *KGB: The Inside Story of its Foreign Operations from Lenin to Gorbachev* (London: Hodder & Stoughton 1990).
Andrew, Christopher, and Mitrokhin, Vasili, *The Mitrokhin Archive II: The KGB and the World* (London: Penguin, 2006)
Andrew, Christopher, and Mitrokhin, Vasili, *The Mitrokhin Archive: The KGB in Europe and the West* (London: Penguin Books, 2000).
Atack, Iain, *The Ethics of Peace and War: From State Security to World Community* (Edinburgh: Edinburgh University Press, 2005).

Bellaby, Ross W., *The Ethics of Intelligence: A New Framework* (London: Routledge, 2014).
Bellamy, Alex J., *Just Wars: From Cicero to Iraq* (Cambridge: Polity Press, 2006).
Bellamy, Christopher, *The Evolution of Modern Land Warfare: Theory and Practice* (London: Routledge, 1990).
Brecher, Bob, *Torture and the Ticking Bomb* (Oxford: Blackwell Publishing, 2007).
Breckinridge, Scott D., *The CIA and the US Intelligence System* (Boulder: Westview Press, 1986).
Callanan, James, *Covert Action in the Cold War: US Policy, Intelligence and CIA Operations* (London: I.B.Tauris, 2010).
Carruthers, Susan L., *Winning the Hearts and Minds British Governments, the Media and Colonial Counter-Insurgency 1944-1960* (London: Leicester University Press, 1995).
Clarke, Richard A., and Knake, Robert K., *Cyber War: The Next Threat to National Security and What to do About it* (New York: Ecco, 2012).
Clarke, Richard, Morell, Michael, Stone, Geoffrey, Sunstein, Cass, and Swire, Peter, *The NSA Report: Liberty and Security in a Changing World* (Princeton: Princeton University Press, 2014).
Clausewitz, Carl von, *On War*, Michael Howard and Peter Paret, edited and translated (Princeton: Princeton University Press, 1976).
Corera, Gordon, *Intercept: The Secret History of Computers and Spies* (London: Weidenfeld and Nicolson, 2015).
Creveld, Martin van, *The Transformation of War: The most Radical Reinterpretation of Armed Conflict since Clausewitz* (London: The Free Press, 1991).
Cruickshank, Charles, *Deception in World War II* (Oxford: Oxford University Press, 1979).
Cullather, Nick, *Secret History The CIA's Classified Account of its operations in Guatemala*, Second Edition, (Stanford: Stanford University Press, 2006).
Daugherty, William J., *Executive Secrets: Covert Action and the Presidency* (Lexington: The University Press of Kentucky, 2004).
Davies, Philip H.J., *Intelligence and Government in Britain and the United States A Comparative Perspective Volume 1: Evolution of the US Intelligence Community* (Oxford: Praeger Security International, 2012).
Davies, Philip H.J., *Intelligence and Government in Britain and the United States A Comparative Perspective Volume 2: Evolution of the UK intelligence Community* (Oxford: Praeger Security International, 2012).
Davies, Philip H.J., *MI6 and the Machinery of Spying* (Abingdon: Frank Cass Publishers, 2004).
Dinstein, Yoram, *War, Aggression and Self-Defence,* Third Edition (Cambridge: Cambridge University Press, 2001).
Dorril Stephen, *MI6: Fifty Years of Special Operations* (London: Fourth Estate, 2001).
Fletcher, George P., and Ohlin, Jens David, *Defending Humanity: When Force is Justified and Why* (Oxford: Oxford University Press, 2008).
Flick, Uwe, *Introducing Research Methodology A Beginner's Guide to doing A Research Project*, Second Edition (London: SAGE Publications, 2015).
Fotion, Nicholas, *War and Ethics: A New Just War Theory* (London: Continuum International Publishing Group, 2007).
Frome, Helen, *The Ethics of War and Peace: An Introduction* (London: Routledge, 2011).

Garnett, David, *The Secret History of PWE: The Political Warfare Executive 1939-1945, with an introduction by Andrew Roberts* (London: St Ermin's Press, 2002).
Godson, Roy, *Covert Action* (Washington DC, Transaction Books, 1981).
Godson, Roy, *Dirty Tricks or Trump Cards: US Covert Action and Counterintelligence* (London: Transaction Publishers, 2006).
Grey, Chris Hables, *Postmodern War: The new Politics of Conflict* (London: Routledge, 1997).
Grove, Eric, *Vanguard to Trident British Naval Policy Since World War II* (Annapolis: Naval Institute Press, 1987).
Handel, Michael I., *Masters of War: Classical Strategic Thought*, Third Edition (London: Frank Cass Publishers, 2002).
Harris, Shane, *@War: The Rise of Cyber Warfare* (London: Headline, 2015).
Helmke, Belinda, *Under Attack: Challenges to the Rules Governing the International Use of Force* (Farnham: Ashgate Publishing Company, 2010).
Hennessy, Peter, *The Secret State: Preparing for the Worst*, Second Edition (London: Penguin Books, 2010).
Howard, Michael, *Studies in War and Peace* (London: Temple Smith, 1970).
Jeffery, Keith, *MI6: The History of the Secret Intelligence Service 1909-1949* (London: Bloomsbury, 2010).
Johnson, Loch K., *Secret Agencies: US Intelligence in a Hostile World* (New Haven: Yale University Press, 1996).
Johnson, Loch K., *America's Secret Power: The CIA in a Democratic Society* (Oxford: Oxford University Press, 1991).
Jomini, Antoine Henri, *The Art of War*, Brig Gen. J.D. Hittle (ed) and translated (New Delhi: Natraj Publishers, 2005).
Kahn, Herman, *On Escalation: Metaphors and Scenarios* (Westport: Greenwood, 1986).
Kaldor, Mary, *New and Old War: Organised Violence in a Global Ear*, Second Edition (Cambridge: Polity Press, 2006).
Kaplan, Fred, *Dark Territory The Secret History of Cyber War* (London: Simon and Schuster, 2016).
Keegan, John, *A History of Warfare*, Second Edition (London: Pimlico, 2004).
Lashmar Paul and Oliver James, *Britain's Secret Propaganda War 1948-1977* (Stroud: Sutton Publishers, 1998).
Libicki, Martin C., *Cyberdeterrence and Cyberwar* (RAND Project Air Force: Santa Monica, 2009).
Lomas, Daniel W.B., *Intelligence, Security and the Attlee Government 1945-1951: An Uneasy Relationship?* (Manchester: Manchester University Press, 2017).
Lowe, Vaughan, *International Law* (Oxford: Oxford University Press, 2007).
Lowenthal, Mark M., *Intelligence: From Secrecy to Policy*, Fourth Edition (Washington, DC: CQ Press, 2009).
Lowenthal, Mark M., *Intelligence: From Secrets to Policy*, Seventh Edition (Washington, DC: QC Press, 2017).
Lucas, George, *Ethics and Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare* (Oxford: Oxford University Press, 2017).
Machiavelli, Niccolo, *The Art of War*, Translated by Henry Neville (New York: Dover Publications, 2006).
Machiavelli, Niccolo, *The Prince* (Oxford: Oxford University Press, 2005).

Mackenzie, William, *The Secret History of SOE The Special Operations Executive 1940-1945* (London: St Ermin's Press, 2000).
Maogoto, Jakson Nyamuya, *Battling Terrorism Legal Perspectives on the Use of Force and the War on Terror* (Aldershot: Ashgate, 2005).
Mears, Ray, *The Real Heroes of Telemark: The True Story of Secret Mission to Stop Hiter's Atomic Bomb* (London: Hodder and Stoughton, 2004).
Miller, David, *Don't Mention the War Northern Ireland, Propaganda, and the Media* (London: Pluto Press, 1994).
Munkler, Herfried, *The New Wars*, Translated by Patrick Camiller (Cambridge: Polity Press, 2005).
Omand David, *Securing the State* (New York: Columbia University Press, 2010).
Perry, David L., *Partly Cloudy: Ethics in War, Espionage, Covert action, and Interrogation* (Plymouth: Scarecrow, 2009).
Pieper, Moritz, *Hegemony and Resistance around the Iranian Nuclear Programme* (Abingdon: Routledge, 2017).
Porch, Douglas, *The French Secret Services: From The Dreyfus Affair to the Gulf War* (Oxford: Oxford University Press, 1997).
Prados, John, *Presidents' Secret Wars: CIA and the Pentagon Covert Operations From World War II Through the Persian Gulf*, Revised and Expanded Edition (Chicago: Elephant Paperback, 1996).
Puddington, Arch, *Broadcasting Freedom: The Cold War Triumph of Radio Free Europe and Radio Liberty* (Lexington: University of Kentucky Press, 2000).
Ragin, Charles C., *The Comparative Method: Moving Beyond Qualitative and Quantitative Strategies* (Berkeley: The University of California Press, 1989).
Richardson, Jeffery T., *The US Intelligence Community*, Seventh Edition (Boulder: Westview Press, 2016).
Rid, Thomas, *Cyber War Will Not Take Place!* (London: Hurst and Company, 2013).
Rid, Thomas, and Hecker, Marc, *War 2.0: Irregular Warfare in the Information Age* (London: Praeger Security International, 2009).
Rositzke, Harry, *The CIA's Secret Operations: Espionage, Counterespionage and Covert Action* (London: Westview Encore Edition, 1988).
Schmitt, Micahel N., (General Editor) and Vihul, Liis, (Managing Editor) *Tallinn Manual 2.0 On the International Law Applicable to Cyber Operations: Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence* (Cambridge: Cambridge University Press, 2017).
Schmitt, Abram N., and James, Gary, *Silent Warfare: Understanding The World of Intelligence* (Washington D.C: University of Nebraska Press, 2002).
Scott, Shirley V., Billingsley, Anthony John, and Michaelsen, Christopher, *International Law and the Use of Force: A Documentary and Reference Guide* (Oxford: Praeger Security International, 2010).
Shakarian, Paulo, Shakarian, Jana, Ruef, Andrew, *Introduction to Cyber-Warfare: a Multidisciplinary Approach* (Amsterdam: Morgan Kaufmann Publishers, 2013).
Singer, P.W., and Friedman, Allan, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford: Oxford University Press, 2014).
Smith, Michael, *The Anatomy of a Traitor: A History of Espionage and Betrayal* (London: Aurum Press, 2017).
Smith, General Rupert, *The Utility of Force: The Art of War in the Modern World* (New York: First Vintage Books, 2008).

Stewart, Brian, and Newbery, Samantha, *Why Spy? The Art of Intelligence* (London: Hurst and Company, 2015).
The Twentieth Century Fund, *The Need to Know: The Report of the Twentieth Century Fund Task Force on Covert Action and American Democracy*, with Background paper by Allan E. Goodman and Bruce D. Berkowitz (New York: The Twentieth Century Fund Press, 1992).
Treverton, Gregory F., *Covert Action: The CIA and the Limits of American Intervention in the Post Cold War World* (London: I.B. Tauris, 1987).
Treverton, Gregory F., *Reshaping National Intelligence for an Age of Information* (Cambridge: Cambridge University Press, 2003).
Tse-Tung, Mao, *The Art of War* (Texas: El Paso Norte Press, 2005).
Tzu, Sun, *The Art of War*, James Clavell (ed) (London: Hodder and Stoughton, 1981).
Walzer, Michael, *Just and Unjust War A Moral Argument with Historical Illustrations*, Fifth Edition (Philadelphia: Basic Books, 2015).
West, Nigel (ed), *The Secret History of British Intelligence in the Americas 1940-1945* (New York: Fromm International, 1999).
Willcox, David R., *The Press and Conflict: The Gulf War and Kosovo* (London: Routledge, 2005).
Williamson, Myra, *Terrorism, War and International law: The Legality of the Use of Force against Afghanistan in 2001* (Farnham: Ashgate Publishing Limited, 2009).
Zegart, Amy B., *Flawed by Design: The Evolution of the CIA, JCS, and NSC* (Stanford: Stanford University Press, 1999).
Zetter, Kim, *Countdown to Zero: Stuxnet and the launch of the World's First digital Weapon* (New York: Broadway Books, 2014).