Intelligence Agencies in Cyberspace:

Adapting the Intelligence Cycle to Cyber Threats and Opportunities

A thesis

submitted in partial fulfilment

of the requirements for the degree

of

Master of Social Sciences

at

The University of Waikato

by

Jedediah Warwick Greenwood

KO TE TANGATA

THE UNIVERSITY OF
WAIKATO
Te Whare Wānanga o Waikato

2020

Abstract

Intelligence has grown and changed dramatically over the past hundred years with the advent of cyberspace. This thesis will begin by examining how the intelligence cycle has adapted to accommodate cyber threats and opportunities, before conducting three national case studies examining the organisational changes in the signals intelligence agencies in New Zealand, the United Kingdom, and the United States of America. It will utilise the analysis of how the intelligence cycle and States have grown to accommodate cyber phenomenon and will conduct two case studies on the recent events concerning Huawei and the hacking of the 2016 US Election. Through this, this thesis will ultimately show that one of the main responses to cyber by intelligence agencies has been increased social engagement, through interaction with the general public in a familiar cyber environment, such as Twitter, in an endeavour to combat the rise in cyber crime by promoting awareness of cyber security issues and ensuring people have the knowledge and means to keep themselves safe in cyber space. This has also involved the monitoring and combatting of extremist propaganda material disseminated online for the purposes of promoting extremist ideologies and indoctrinating vulnerable people.

Acknowledgments

I would like to thank my supervisor Dr Joe Burton, whose expert guidance and advice has been essential for writing this thesis, something for which I am immensely grateful.

I would also like to thank my partner for all his patience, support, and encouragement during my studies here.

Declaration

- This thesis is ready for examination
- The thesis embodies the student’s own work, carried out under my direct supervision
- Ethical approval is not required

J Burton

Dr Joe Burton
Joe.burton@waikato.ac.nz

Contents

Introduction

Within the emerging field of cyber there has been a significant restructure of national intelligence communities globally. Alongside their foreign counterparts in more well-known agencies such as the British Government Communications Headquarters (GCHQ) signals intelligence was initially tasked with accessing foreign communications. With the advance and rise of the internet and digital communications, the role of signals directorates has greatly transformed to adapt to this new phenomenon. Over recent years some of the more pressing implications of this have emerged, whereby this has significant implications for the task of counter-terrorism, where individuals who are possibly at risk of radicalisation can be identified and monitored.

In exploring the question of how intelligence agencies are adapting to cyberspace, this thesis will show that one of the biggest changes within intelligence has been with the pursuit of social engagement to combat the diverse and dynamic threat that is posed by malicious cyber actors. Social engagement can be seen as the process where Agencies will participate in connecting with the wider public via a digital platform, such as Twitter. Such engagement here is an important tool as it allows the Agencies to effectively provide information about cyber security and helps to provide an appearance of transparency in the organisation.

Using the Intelligence Cycle as a conceptual tool, the first section will discuss what this is and how it has evolved and developed over the years to incorporate cyber. The evolution of this has been necessary for intelligence agencies to keep pace with developments in communication and helping to provide them with a platform to protect the State from the cyber threat in the 21st Century.

Using the recent changes in the intelligence agencies in New Zealand, the United Kingdom, and the United States of America as national case studies, the next sections will show how they are respectively adapting to cyber. These three States were chosen as, while they are all Western democracies and are part of the intelligence sharing alliance known as Five Eyes, they have all had markedly different responses to cyber security but have arrived at somewhat similar outcomes. Ultimately I show that the major changes, which in most cases were a common theme among the three nations, were legislation reform allowing agencies to keep up pace with advances in cyber; embracing new forms of social media and engagement with the general public as a means of promoting cyber security and protecting the economic interests of the State; significant investment in specialised cyber divisions focused on major cyber security threats; and the development of offensive cyber capabilities to provide both a deterrence to targeted foreign cyber hostilities and as a means of pursuing targets to mitigate their operational effectiveness.

Next will be an examination of some of the main issues that have been posed by cyber and the response by intelligence agencies. This will begin with a discussion of the Tallinn Manual and the importance of this endeavour to engage international law on the topic of cyber. Two of the main issues posed by cyber are the encroachment on the right to privacy, and the attempts at undermining public development of military-grade encryption technologies.

Lastly it will discuss two case studies on cyber and how intelligence agencies have been able to respond here: the Huawei scandal and the US election hack. Both events are important in representing two very different politically charged situations, with the Huawei scandal accusations of the company being used by Chinese intelligence for international espionage, and the election hack involving state-sponsored Russian hackers influencing the outcome of the 2016 US election campaign. These two case studies are also interesting in that they use the US national case study to address the topic of how the intelligence cycle has adapted to the increased cyber threat.

1. Introducing the Intelligence Cycle as a Conceptual Tool

The Cambridge University Press Dictionary defines intelligence as "the ability to learn, understand, and make judgements or have opinions that are based on reason[1]". Within such a definition, intelligence requires understanding of the subject matter, how any new information relates to it, and using that information to generate a belief about something. The process that is used here for this is known as the Intelligence Cycle. The Intelligence Cycle has five main areas: Direction, Collection, Collation, Interpretation, and Dissemination.

Modern intelligence underwent a dramatic transformation during the Second World War, where advances in technology and the increased need for quick, reliable, and secure communications prompted a variety of changes, and created several new Agencies, many of which were the precursor to the present-day communications intelligence agencies.

Such necessary advances here included the increased adoption of cryptographic cyphers for securing diplomatic and military communiques, and the need for faster means of communication – not knowing what the enemy was doing, or what the State wanted you to do out of real-time was a deeply pressing issue. Communication technology had the power to sway victory into the hands of those who could transmit and receive information with little delay.

Furthermore, another significant evolution in intelligence was precipitated by the devastating attacks against the United States of America on September 11, 2001, by the terrorist network Al Qaeda. This event was significant in that it marked a changing point in the level of threat posed to a Western state by a non-state actor – something quite critical in the post-Cold War era.

While non-state and state-sponsored actors had posed significant threat to the State before, this was typically thought of as an issue belonging more to 'non-Western' states, such as Afghanistan. The events of September 11 showed an increase in the reach of non-state actors, bursting the imagined 'bubble' of security. Since this event there had been several other highly publicised attacks, including the bombings in Bali in 2002 and London in 2005. Such incidents resulted in a transformation of the intelligence community and state security agencies around the world with the then-U.S. President George W. Bush signing the Homeland Security Act 2002 and Congress passing the USA PATRIOT Act. Furthermore, Australia passed the *Anti-Terrorism Bill (No. 2) 2005* once-again outlawing sedition[2], and Canada adopted anti-terrorism laws for the first time[3].

Regarding this, Anton states that "The rapid evolution of all forms of risks and threats has led to a complete analysis of the entire spectrum of national and/or alliance/coalition security. In this respect intelligence structures have become more dynamic and flexible, adapting quickly to counter both direct and indirect risks and threats[4]". John Keegan also notes something similar, stating that systems do not change unless circumstances change[5].

In addition to September 11 being a pivotal tipping point for intelligence organisations and national security, the term 9/11 itself has become synonymous with a catastrophic event that occurs almost as a

[1] Cambridge University Press. (2019). *Intelligence*, https://dictionary.cambridge.org/dictionary/english/intelligence

[2] Lynch, A., McGarrity, N., & Williams, G. (19 February 2015) *Australia's Response to 9/11 Was More Damaging to Freedom Than Any Other Country's*, The Guardian, https://www.theguardian.com/commentisfree/2015/feb/19/australias-response-to-911-was-more-damaging-to-freedom-than-any-other-countrys

[3] MacLeod, I. (16 January 2015). *Canada's Post 9/11 Anti-Terror Laws*, Ottawa Citizen, https://ottawacitizen.com/news/national/canadas-post-911-anti-terror-laws

[4] Anton, C. (2015). Intelligence Cycle Planning in Military Coalition Operations, *Journal of Defense Resources Management*, *6*(1), pp. 133-136, p. 135

[5] Keegan, J. (2003). *Intelligence in War: Knowledge of the Enemy from Napoleon to Al-Qaeda*, Penguin Random House.

result of complacency. Terms here such as ‘cyber 9/11’ or ‘cyber Pearl Harbour’ are used to describe the threat posed by a cyber attack, where a series of events, such as the mis-interpretation of intelligence, failure to recognise the value or importance of intelligence, and the exploitation of security flaws and vulnerabilities can lead to devastating consequences – an event which, in hindsight should been prevented but all warning signs were ignored or downplayed because it was so unlikely to occur.

With regards to September 11, there was intelligence during the 1990’s that indicated a plan to hijack civilian aircraft. However, the remoteness of this happening and the focus of intelligence agencies on other issues meant that this was not acted upon. This was a similar situation with Pearl Harbour, prompting a likely theory that this was intentionally not acted upon to entice the attack, thus allowing the United States to enter the Second World War with the support and approval of Congress and the American public.

The Intelligence Cycle is a useful formula for the production of intelligence, allowing the State to make an informed decision, although care must be taken to prevent the ‘politicisation of intelligence’, and the use (or misuse) of intelligence to advance a political agenda. O’Brien refers to the ‘politicisation of intelligence’ as “the inappropriate use of the intelligence process, intelligence collection assets or intelligence-related material for party political purposes … political misuse of intelligence taking a variety of forms, occurring at all stages of the intelligence cycle and taking place within intelligence agencies[6]”. It is for this reason that it is essential for intelligence agencies to be politically neutral, for their purpose to be solely for the defence of the State.

A prime example of the failure of intelligence can be seen with the case of the former Soviet leader Joseph Stalin. Stalin represented “the ultimate nightmare for the intelligence officer: a commander who chooses to suppress the very best intelligence handed to him on a plate, because he has his own agenda, and is prepared to go to any lengths to prevent the truth becoming known, much less acted upon[7].” On June 22, 1941, German forces broke their alliance with their Communist allies, crossing the border and launching the ill-fated invasion of Soviet Russia. Despite having been presented with intelligence showing that Germany was looking eastwards for expansion, Stalin refused to accept this as it did not fit his agenda and interfered with his plans. Instead of accepting this and adapting, he purged the Soviet military of the majority of its officers – some “seventy-five of the eighty members of the Military Soviet … every commander of every military district: two thirds of the divisional commanders, half the brigade commanders and over 400 of 456 staff colonels[8]” were killed due to fears of ‘internal enemies’. Stalin knew that military confrontation was inevitable, having been presented with irrefutable evidence, but due to him not being ready for it refused to accept any intelligence showing him what he did not want to hear, resulting in millions of casualties.

The above case helps to highlight the necessity for intelligence agencies to be politically neutral and removed from the politicisation of governments and have independent oversight. Typically, this separation is frequent in a more ‘democratic’ nation and much less so in a less ‘democratic’ nation, such as an autocracy, where there is little or no division of power. The intelligence cycle is particularly useful here in, among other things, determining the value of a potential threat that has been identified, with each of the five stages (direction, collection, collation, interpretation, and dissemination) playing a vital role.

[6] O’Brien, C. (2007). Politics of Intelligence: How the Politicisation of the Intelligence Cycle Undermines the Integrity of Australia’s Intelligence Agencies, *Journal of the Australian Institute of Professional Intelligence Officers, 15*(3), pp. 58-68

[7] Hughes-Wilson, J. (2016). *On Intelligence: The History of Espionage and the Secret World,* Constable. P. 232.

[8] Ibid, p. 231

Direction

The core ideal is that there is a need for an intelligence assessment to be undertaken, something that "should be driven by information requirements specifically needed for threat assessment and threat management, and the early detection of warning behaviours[9]".This could be in the form of a question that the State needs addressing, for example. The need for an intelligence assessment should also be driven by legitimate necessity for advancing security, and not driven by internal politicking or for political reasons, as the case of Australia in 1999-2001 highlights.

Between July 1999 and December 2001 there was a brief increase in the number of arrivals to Australia via boat, prompting the 'Maritime People Smuggling to Australia' threat to be the highest priority for the National Foreign Intelligence Assessment Priorities. Due to the potential for terrorists arriving in Australia as asylum seekers, this has prompted the high level of response, despite the possibility of this actually being extremely low, with Dennis Richardson, the then-Director General of the Australian Security Intelligence Organisation Director General, questioning "Why would people (associated with international terrorism) use the asylum seeker stream when they know they will be subject to mandatory detention?[10]"

O'Brien furthers this by citing immigration figures showing that eighty-four percent of asylum seeker applications in Australia are granted, which would lend credence to the notion here that the threat level raised by attempted people smuggling was somewhat over-inflated, intending to "benefit the current government's high profile stand against maritime arrivals rather than the relative nature of the threat[11]". By raising the threat level in response to this for political gain, such as increased polling figures, they ultimately de-valued the threat of other serious issues, such as drugs and arms smuggling, potentially undermining efforts underway to curb this threat. Within cyber the undermining of the threat posed by hostile foreign actors could ultimately mean the difference between a preventing a major cyber attack and allowing it to take place.

To this extent, O'Brien states that "Any political efforts to explicitly interfere with the writing of intelligence reports inherently challenges the absolutely fundamental requirement for intelligence agencies to be independent from the political process … The principle that intelligence agencies must remain free to exercise complete autonomy when determining intelligence assessments underpins the integrity of the entire intelligence process[12]."

The New Zealand Ministry of Foreign Affairs and Trade outlines the biggest security threats facing the world today as being terrorism, the use of weapons of mass destruction, cyber security, people smuggling and trafficking, and space security. Within cyber security, such threats include cyber espionage, cyber terrorism, cybercrime, and cyber vandalism (or 'hacktivism')[13].

One of the main impacts on the direction phase of the intelligence cycle that cyber has had is in the nature of the threat assessments requested. With the New Zealand Government Communications Security Bureau, one of the biggest impacts in the direction phase can be seen with the intentions of the agency. The first publicly published Annual Report, in 2003, addresses the focus of the GCSB as being largely focused on intelligence collection through signals interception, ensuring the integrity of official information, and "assisting in the protection of the national critical infrastructure from

[9] Malone, R. (2015). Protective Intelligence: Applying the Intelligence Cycle Model to Threat Assessment, *Journal of Threat Assessment and Management*, *2*(1), pp. 53-62, p. 55

[10] O'Brien, C. (2007). Politics of Intelligence: How the Politicisation of the Intelligence Cycle Undermines the Integrity of Australia's Intelligence Agencies, *Journal of the Australian Institute of Professional Intelligence Officers*, *15*(3), pp. 58-68, p. 62

[11] Ibid, p. 62

[12] Ibid, p. 59

[13] Ministry of Foreign Affairs and Trade. (2019). *International Security*, https://www.mfat.govt.nz/en/peace-rights-and-security/international-security/

information-borne threats[14]". Through the analysis of the Annual Reports we can see that the nature of the requirement for intelligence assessments have changed with the advance and evolution of cyber.

One of the main focuses in 2003 was the 'War on Terror', increasing the number of analytic and processing staff to address the growing number of trans-national and regional security issues. The 2003 Annual Report states that the Bureau has two main objectives: to ensure that New Zealand's "interests are protected and advanced through the provision of relevant, timely and accurate foreign intelligence, and threat warning intelligence[15]", and that official information and critical national infrastructure is protected.

The 2011 Annual Report saw a marked difference from the previous reports. Previously the Annual Reports showed the GCSB contributing towards increased national and international security, prevention of terrorism and major criminal activity, improved Government decision making and planning, and economic performance. The 2011 Report, whilst still mentioning improved security and economic performance, now also stated a focus on developing cyber capability and maintaining support for military operations. Likewise, the 2018 Report shows further changes in direction, focusing more on cyber rather than providing support for other operations. For example, in response to the increased use of cyber by terrorist and extremist actors internationally, the Report notes that the GCSB, in cooperation with other Agencies, is working to reduce and stop the spread of extremist propaganda online, noting that "The online proliferation of extremist content and ideologies remains a threat to the safety of New Zealanders. Such material is accessible in New Zealand, and is known to be read and distributed by New Zealanders[16]".

In a large way here the effect of cyber on the direction phase has been the increased focus on cyber phenomena.

Collection

The collection phase refers to the gathering of information relevant for the investigation that has been outlined in the direction phase. The various forms of intelligence tend to fall in one of several categories: human intelligence (HUMINT), imagery intelligence (IMINT), signals intelligence (SIGINT), and, more recently, open source intelligence (OSINT).

Human intelligence refers to the use of other people as intelligence sources, through the recruitment of agents, etc, and is the oldest method of intelligence collection. Invoking images of historical spymasters such as Thomas Cromwell and Francis Walsingham, the field of human intelligence is now governed by formal agencies such as the British MI6, the Israeli Mossad, and the New Zealand Security Intelligence Service, to name a few.

IMINT, or imagery intelligence, is the use of imagery or video footage. Imagery intelligence provides a great deal of visual evidence about a target, such as a potential terrorist training camp, but does not provide any context. Imagery intelligence is, in addition to human intelligence, one of the oldest means of intelligence collection. Historically this has been through the use of drawings, sketches and pictures to assess a target or location of interest. Modern technology now allows for the use of accurate photography taken from satellites, infrared imagery, and video footage from drones, to name a few.

Signals intelligence, or SIGINT, is intelligence that is obtained from communications. This includes communications interceptions from wiretapping phones, the code-cracking work at Bletchley Park, etc.

[14] Government Communications Security Bureau. (2003). *Annual Report for the Year Ended 30 June 2003*
[15] Ibid
[16] Government Communications Security Bureau. (2018). *Annual Report for the Year Ended 30 June 2018*

Lastly, of the four main intelligence categories is OSINT, or open source intelligence, which refers to anything in print or electronic form that is publicly available. This includes newspapers, radio and television broadcasts, the Internet, journals, etc. It is in this category that much of the intelligence is typically collected, and is not without its potential issues, such as with false information being printed with the intention of misleading an adversary.

It is within the collection phase of the intelligence cycle that there has been much discussion in the media in recent years, particularly with allegations of mass surveillance and illegal activities by intelligence specialists and contractors. It is not just the intelligence that is collected that is of note here, but also the way in which the collection was carried out. Cyber has had a huge impact on how intelligence is collected, allowing for the taking of extremely high resolution photographs and video footage from satellites and drones, the latter of which has proven to be relatively successful, if highly controversial, at conducting targeted missile strikes. Additionally, cyber has revolutionised how we communicate – no longer through hard-wired telephone lines which can be physically intercepted, but now through encrypted SMS messages, video conferencing through digital platforms, forums, and cloud-based servers, to name a few.

It is also important to note here that the human element is a significant factor in cyber, where errors of judgement, or downright ineptitude, can be a huge boon to intelligence agencies. One example to highlight the impact of cyber on the collection phase of the intelligence cycle is in the case of Mark Taylor, who became known as the ‘bumbling Jihadi’ for incidentally revealing several prominent ISIS locations. Taylor, a New Zealand citizen, moved to Syria in 2014 to join the Islamic State of Iraq and the Levant. The following year, using the Twitter handle ‘Kiwi Jihadi’, he had forgotten to turn off the geotagging function when posting messages, revealing several Islamic State locations[17].

Since its inception in the 2000s, social media has rapidly become a powerful tool for influencing people. There were hundreds of thousands of ‘fake’ accounts created on Facebook and Twitter by hostile foreign actors during the 2016 US Presidential Election, spreading misinformation about Presidential candidate Hillary Clinton. Terrorist and extremist groups also have a strong network on social media, using this to recruit new followers and sympathisers – and encouraging ‘lone wolf’ style attacks in their countries, contributing to the rise of violent attacks by home-grown extremists in the United Kingdom, for example. Additionally, the platforms are used for spreading propaganda and hate messages and showing video footage of the conflict, such as the infamous beheading scenes. Social media here can be both a help and a hindrance to intelligence agencies. On one hand agencies are able to see some of the tactics used by these groups in recruit new members and generate sympathy, and to see who is following them and discussing this online, enabling them to track movements and individuals. On the other hand, while it allows for gathering of intelligence, the messages are still being spread. While there have been some attempts by Facebook and Twitter to shut down various pages and users when they are notified, it doesn’t prevent it from being posted in the first place, and has the very real effect of vulnerable individuals being influenced and indoctrinated. Here social engagement also becomes an important concept, where intelligence agencies can actively work to not only shut down offensive and hostile content, but can engage with the public in a familiar setting, like Twitter or Instagram, to discourage sharing of such content and even refute the messages being portrayed.

Collation

Collation refers to the act of bringing all the intelligence together, sorting through it, and collating it into a database that is ready for analysis. This is an important step as it helps to “mitigate natural biases that occur when considering more information than can be held in working memory at one time. Otherwise, is it easy to fall victim to confirmation bias, the availability heuristic, the fundamental attribution error, and other well-known cognitive biases when evaluating complex

[17] Hurley, B. (13 October 2019). *Police build case against ‘bumbling Jihadi’ Mark Taylor, but outdated anti-terrorism laws could see him walk free*, https://www.stuff.co.nz/national/116471644/police-build-case-against-bumbling-jihadi-mark-taylor-but-outdated-antiterrorism-laws-could-see-him-walk-free

information from disparate sources[18].” Within this section alone the use of computers has allowed for rapidly recalling enormous databases of information and sharing and accessing this remotely from multiple locations. In contrast, for example, in the aftermath of the Second World War, Colonel Reinhard Gehlen was recruited by the United States due to him having “collated the best card index and records on the Eastern Front … After all, a unique, well collated, accurate and up-to-date intelligence database can overcome almost any scruples[19]”.

Modern technology has had a significant impact on this, with the ability to store huge amounts of data on small, portable hard drives, even remote storage accessible via the ‘cloud’. Being able to recall the information in an instant, and via almost any networked device has revolutionised the way in which databases are managed at every level. This does however have several significant issues. Firstly, there are vulnerabilities with storing information digitally. Same as with physical storage, the information is vulnerable to being stolen or copied. However, where physical storage requires physically accessing to the information, digital storage is vulnerable to being hacked from anywhere in the world, and hard drives will eventually fail.

Additionally, there is an issue with having more information than can be processed and used. Again, while this is not an issue solely associated with cyber, it is somewhat magnified as a result. For example, during the Vietnam War the United States military took aerial photographs every time they had a chance, resulting in desk drawers full of pictures that were never once looked at as they were quickly outdated and surplus to requirement. Similarly, within cyber there is still a staggering amount of information collected that could be considered surplus to requirement. In 2018, for example, the New York Times cites a National Security Agency report which stated that the metadata of more than 534 million phone calls and text messages, utilising American telecommunications providers, had been gathered by the NSA. As an aid in the surveillance of someone potentially involved in terrorism only a relatively small amount of this data is actually used, the rest being surplus to requirement[20].

Cyber has a highly pronounced effect on the collation aspect of the intelligence cycle. It is possible to have multiple databases available to recall information instantly, allowing for context to be applied to any new incoming information, based on information previously gather and analysed. The whistleblowing by Edward Snowden helps to provide a prominent example of the impact that cyber has had on the collation phase. John Hughes-Wilson states that the initial founding purpose of the American National Security Agency was to focus on foreign communications intelligence. The events of September 11, 2001, however, generated a renewed interest in the NSA monitoring potential terrorists’ phone and email communications, for which they required the assistance of phone companies and Internet service providers. It was the eventual mission creep that led to the Agency collecting the metadata of millions of American citizens’ communications.

Interpretation

Utilising the HUMINT, IMINT, SIGINT, and OSINT gathered in the collection phase, the interpretation phase of the intelligence cycle is where the analysis is made, drawing a response to the reason why there needed to be an intelligence assessment made in the first place[21]. As was noted in the collection phase, care needs to be taken to not be drawn in with false information and misleading evidence. In analysing the intelligence gathered, the analyst, where pragmatically possible, utilises their sources to corroborate the information – although care must still be taken as it is possible to have a human source corroborate intelligence that was broadcast on the radio, for example, but have

[18] Malone, R. (2015). Protective Intelligence: Applying the Intelligence Cycle Model to Threat Assessment, Journal of Threat Assessment and Management, 2(1), pp. 53-62, p. 54.

[19] Hughes-Wilson, J. (2016). *On Intelligence: The History of Espionage and the Secret World*, Constable. P. 62

[20] In targeting 42 people in 2016, the NSA collected metadata for more than 151 million phone records. Savage, C. (2018). *N.S.A. Triples Collection of Data from U.S. Phone Companies*, https://www.nytimes.com/2018/05/04/us/politics/nsa-surveillance-2017-annual-report.html

[21] Malone, R. (2015). Protective Intelligence: Applying the Intelligence Cycle Model to Threat Assessment, Journal of Threat Assessment and Management, 2(1), pp. 53-62

everything converging backward upon a single source, such as a newspaper article. Great care must be taken in the interpretation phase of the intelligence cycle, with John Hughes Wilson noting "If a defeat caused by a catastrophic failure of intelligence … then paradoxically a great victory assisted by brilliant intelligence can lead to complacency and an intelligence disaster further down the line[22]".

Loch Johnson has identified 8 key attributes for an effective intelligence analysis: accuracy, relevance, timeliness, comprehensiveness, readability, probability, objectivity, and actionability. With this, for an intelligence report to fulfil its requirement the information contained within it must be accurate and relevant, reporting on whether a building is used as shelter for displaced civilians or as a safehouse for an arms dealer, for example, and also be current – if the building was a safehouse six months ago but has been abandoned then it may not be considered relevant to an arms dealers current location. It must also be comprehensive and readable, providing all the information required to make a decision, and also engaging to keep the attention of busy policymakers. With probability and objectivity, it needs to state the possibility of an anticipated event occurring and is not framed in such a way as to achieve a specific outcome – intelligence needs to be impartial. Lastly, intelligence reports should be actionable – that is, they should achieve their purpose and allow policymakers to take action accordingly. Johnson notes here that 'Chatter' about terrorist planning is better than no information at all; but precise dates and times … are infinitely more helpful. In 2001, Washington leaders knew about the threat of aerial terrorism; what they did not know is that 19 hijackers were going to board American commercial airliners on the morning of 9/11, with the objectives of flying the planes into the World Trade Centre[23]."

Dissemination

Lastly, the dissemination phase refers to the distribution of the intelligence assessment to those who initiated the requirement for it. Within this it is crucial that the intelligence assessment contains accurate information and is not designed to sway the opinion of its audience towards a bias. As this can have a direct impact on policy and dictate the response of governments, there is a necessity for intelligence assessments to be politically neutral and free from a political agenda. Being able to receive intelligence in 'real time' is, in addition to the accuracy of the intelligence, one of the most critical aspects. During the Second World War, the teams at Bletchley Park worked tirelessly in cracking German codes, but this was a slow process, where "only about half of all intercepts were read, many of them too late to provide practical assistance"[24]. Following the dissemination phase, the cycle returns to the initial direction phase, whereby if the intelligence assessment raises additional questions then a follow-up investigation needs to be done and so on.

The dissemination phase can also refer to the sharing of intelligence with allies (or adversaries), and may involve the intentional sharing of mis-represented intelligence, to lead the audience to specific conclusion (it is for this reason that intelligence domestically should necessarily be free from 'politics'). An example of this is during the First World War. During their attempts to stay neutral, the United States of America allowed Germany to send diplomatic cables through their diplomatic channels. The United Kingdom had cut German telegraphic cables rendering them otherwise incapable of communicating with North and South America. The United Kingdom had broken the US diplomatic cables and was reading the messages being sent, discovering the German plan to betray the American hospitality. Should Mexico ally itself with Germany then a victorious Axis power would offer them Texas, New Mexico, and Arizona. The issue posed to the United Kingdom here is how to inform the neutral Americans without revealing that they were reading their diplomatic cables.

The Admiralty managed to acquire a copy of the message in Mexico City, then show this to the US Embassy in London, hinting that they had come about it via a well-placed informant, and leak it to the US press. The result was it became a front-page story across all major US newspapers, and the US

[22] Hughes-Wilson, J. (2016). *On Intelligence: The History of Espionage and the Secret World*, Constable. P. 205
[23] Johnson, L. (2011). National Security Intelligence in the United States: A Performance Checklist, *Intelligence and National Security*, *26*(5), 607-615, p. 611
[24] Hastings, M. (2015). *The Secret War: Spies, Codes and Guerrillas 1939-1945*, William Collins. P. 72

declaring war on Germany two months later. Had the United States learned at the time that the British had broken their cables then it would have been a diplomatic disaster. Similarly, had Germany realised that their messages were being read then their means of communication would have been changed immediately[25]. As with modern encryptions, once a system has been broken it can no longer be trusted.

One significant impact that cyber has had on the dissemination phase is in the speed with which information can be transmitted. Technology has had a great effect on the intelligence cycle, with the advent of signals intelligence and imagery intelligence, and through the widespread use of the Internet, on open source intelligence also. With thousands of discussion boards, news media websites, social media, and video imaging platforms available at a moment's notice, modern technology and the rise of cyber have made it easier than ever to engage socially in a globally connected world. Most pressing has been with a global increase in our use of the Internet, this has created multiple digital platforms for terrorist organisations and networks to share propaganda images and videos, generating sympathy and support around the world.

An underlying theme that does emerge is that no process is perfect, but that by constantly re-evaluating and adapting to changing technology and demands then the process can at least be better than it was. The intelligence cycle, whilst an effective tool for conducting an intelligence assessment, is not perfect or infallible, and as has been shown is vulnerable to politicisation and misrepresentation of intelligence, resulting in (or even because of) intelligence failures potentially causing significant harm. It is for this that increased transparency, as much as could be expected of an agency dependent upon secrecy, is essential for its continued success. With such increasingly connected global social networks, social engagement with the wider public is essential in keeping the State secure, in providing a trusted platform for disseminating cyber security awareness and improving trust in the organisation (which is a key attribute for a democracy). Having discussed the intelligence cycle, this thesis now turns to the three national case studies, which will further build upon the key points that this section has introduced – social engagement and institutional changes adapting to cyberspace.

[25] Government Communications Headquarters. (25 January 2019). *Real World Impacts: How GCHQ's predecessors contributed to the US entering World War I*, https://www.gchq.gov.uk/information/century-how-work-gchqs-predecessors-contributed-us-entering-world-war-i

2. New Zealand Cyber and Intelligence

In their report *Intelligence and Security in a Free Society,* Dame Patsy Reddy and Sir Michael Cullen note that within New Zealand there is a generally held public idea that as a nation we are relatively safe and sheltered from some of the more extreme threats facing our allies elsewhere in the world[26]. Previously any association with the word 'terrorism' and 'New Zealand' had been used to refer to Mark Taylor, or in a more general sense to refer to our counter-terrorism efforts overseas. Media reporting had likewise been critical of the idea that a terrorist act could occur in New Zealand. A leaked memo from the New Zealand Defence Force in 2016 had warned that a terrorist attack in New Zealand was only a matter of time, although this was referring more with regards to Islamic extremism targeting Defence Force personnel. In 2019 a terrorist incident in New Zealand did occur, targeting the Christchurch Muslim community as they went for afternoon prayers.

On 15 March 2019, Brenton Tarrant opened fire on the Al Noor Mosque and the Linwood Islamic Centre in Christchurch, killing 51 people and wounding dozens more. The atrocious terrorist act, motivated by extreme Islamophobia and white supremacy, drew international condemnation and offerings of support for those affected, in addition to criticism of New Zealand's Intelligence Community (NZIC). In the days following the attack questions began to be asked around why and how New Zealand's domestic agencies had no prior knowledge about his extremist views and how could the attack have come about with no indications or warnings. In the immediate aftermath of the attack, the core NZIC agencies (the GCBS and the SIS) immediately received an increase in funding with the terror threat level being raised to 'high' for the first time in national history (although this was downgraded to 'medium' on 17 April 2019). With regards to the question of why New Zealand's national intelligence agencies were not monitoring Tarrant, threats from white nationalism was not something that was being actively monitored as closely as other more pressing threats facing the nation, such as people smuggling, for example.

In a similar situation as the 9/11 attacks in New York, Christchurch has shown how devastating a single incident can be in causing a global reaction. What long-term implications this has for New Zealand's domestic security strategy remains to be seen. What this event does show, however, is that even if a suspect is active on various extremist chatrooms and forums, there is no guarantee that this will be noted by an intelligence agency or relayed to their international partners. Whilst the ability to operate in cyberspace does have many advantages, particularly with the intelligence cycle and allowing for more information to be recalled with quicker turnaround, it is not an infallible process – intelligence can be overlooked, misreported and misinterpreted. The following study of intelligence reform in New Zealand shows how the community has evolved through making mistakes and adapting to operate more efficiently in the digital age and providing advanced cyber capabilities.

Kitteridge Report

The first major analysis of a New Zealand intelligence agency came from the *Review of Compliance at the Government Communications Security Bureau*[27] (otherwise known as the 'Kitteridge Report'), which was conducted by the now-Director of the SIS Rebecca Kitteridge. Commissioned to investigate allegations of severe misconduct and illegal spying conducted by the GCSB, the report found that while errors had been made, these had come about as a result of misinterpretations of the GCSB Act 2003, and not as an act of malice. As a result, one of the key recommendations of the report is legislative reform to clarify the legislation and to implement a compliance framework.

Kitteridge also noted that in an organisation such as the GCSB, where they possess such intrusive powers and capabilities, there is an essential need for external oversight and accurate interpretations of the legislation surrounding these abilities. The report found that the Bureau had no effective internal auditing, inadequate oversight, and was misinterpreting the GCSB Act 2003. The

[26] Cullen, M. & Reddy, P. (29 February 2016). *Intelligence and Security in a Free Society: Report of the First Independent Review of Intelligence and Security in New Zealand*

[27] Kitteridge, R. (March 2013). *Review of Compliance at the Government Communications Security Bureau*

misinterpretations here were caused by vagueness in the wording of the legislation and of it not being fit for purpose. Kitteridge further notes that:

> "Technology is changing enormously … the nature of the communications media being intercepted at various stages of GCSB's existence (high frequency radio, then microwave via satellite) meant that communications being targeted for foreign intelligence purposes could mostly be readily distinguished and intercepted. That has largely changed with the technological switch to ubiquitous use of the Internet. The GCSB Act was intended to be technology-neutral and future-proofed, but with the benefit of hindsight it looks to be rather narrowly focused on the SIGINT function as it operated in 2003 … it has not kept pace with developments, especially in relation to information assurance and cyber security.[28]"

When the Act was created the technological landscape was drastically different compared with today. To highlight how far technology has come since the inception of this Act, the social media site MySpace was founded in 2003, the original Xbox gaming console had been released just two years prior in 2001, and the dotcom bust of the early 2000s was still very recent. Since this time MySpace has risen and fallen, surpassed by several variants and the meteoric rise of Facebook which has rapidly become a permanent fixture in many peoples' lives even in the wake of the revelations of immense privacy breaches, such as Cambridge Analytica. Furthermore, the first iPhone was not due to be released until 2007, four years after the GCSB Act 2003, and smart phones have come to revolutionise how we communicate. We have gone through two additional generations of video game consoles, and access to the internet has arguably become essential for life.

The failure of policy to adapt and change as technology has evolved is hardly a situation unique to the GCSB, with Lucas Kello noting that "the cyber revolution gives rise to novel threats and opportunities requiring immediate policy responses; yet understanding its nature and its consequences for security is a slow learning process[29]". In addition to the failure of policy and an organisational response to cyber, there had been seemingly innocuous decisions at the individual level that contributed to severe misunderstandings and implementations of the legislation. Kitteridge notes that GCSB staff had been storing compliance advice on their personal drives, meaning that only the individual staff member had access to the file, which they were using as an aid to the application of the legislation. This resulted in using outdated opinions or advice. The recommendation Kitteridge gave here is that such information should be controlled by the legal staff responsible, and continuously updated where required[30].

Intelligence and Security in a Free Society

Following on from the Review of Compliance report was *Intelligence and Security in a Free Society*, by Sir Michael Cullen and Dame Patsy Reddy. Published in 2016, the report advocated strongly for a single, cohesive Act that would clearly dictate the functions of the various agencies. Noting that, in the aftermath of the report by Rebecca Kitteridge, the GCSB had taken a much more conservative stance in their interpretation of the legislation, resulting in the Agency not operating as effectively as they could have been, for fear of inadvertently violating the GCSB Act 2003[31].

The Report was to assess "whether the legislative frameworks of the Agencies are well placed to protect New Zealand's current and future national security, while protecting individual rights; whether the current oversight arrangements provide sufficient safeguards at an operational, judicial and political level to ensure the Agencies act lawfully and maintain public confidence; whether the legislative provisions arising from the Countering Foreign Terrorist Fighters legislation, which

[28] Ibid, p.24.

[29] Kello, L. (2013). The Meaning of the Cyber Revolution: Perils to Theory and Statecraft, *International Security*, *38*(2), pp.7-40, p.7

[30] Kitteridge, R. (March 2013). Review of Compliance at the Government Communications Security Bureau

[31] Cullen, M. & Reddy, P. (29 February 2016). *Intelligence and Security in a Free Society: Report of the First Independent Review of Intelligence and Security in New Zealand*.

expires on 31 March 2017, should be extended or modified, and; whether the definition of 'private communication' in the legislation governing the GCSB is satisfactory[32]".

The Report notes that it was immediately apparent that the legislation governing the Agencies was not fit for purpose, with a significant lack of clarity in the GCSB Act 2003, meaning that the Agency was not able to operate as effectively as it could be. Additionally, the GCSB Act 2003 was not harmonious with the New Zealand Security Intelligence Service Act 1969, resulting in a lack of cooperation between the two Agencies[33].

They also note that recent international controversies have incited reviews of intelligence gathering techniques by other democratic countries, although these "to a greater extent than ours, have been conducted against a backdrop of heightened awareness of a very real threat of terrorism … Each country has taken a different approach, influenced by the values of its citizens, its political institutions and its recent and historical experiences[34]".The approaches taken by the United States in the wake of events such as 9/11, for example, are drastically different from that taken by the United Kingdom following the London bombing in 2005, and again compared with New Zealand following the Mosque shooting in March 2019. All three incidents were devastating terrorist attacks which had a dramatic impact on the international community but were followed by markedly different responses domestically.

Within this there is also a great deal of difference in how the public view the trade-off between privacy and security. In discussing this, Cullen and Reddy note that, in 2014, most people surveyed in the United Kingdom could support a loss of privacy if it meant a reduction in the threat posed by extremists and violent criminals. During the same time period, however, more than 50 percent of New Zealanders surveyed found surveillance by Government agencies concerning (although less than 10 percent could name both of New Zealand's intelligence and security agencies). Regarding this, Cullen and Reddy note that there is a need for the Agencies to be more open about their work and the necessity for this to ensure national safety and security[35]. To be considered here, however, was that during this time period the United Kingdom had experienced a recent terrorist attack, whereas New Zealand had not. The first-hand experiences with violent extremism could explain the marked differences in the attitudes towards privacy and security in their respective states.

Lastly, one of the main points noted in the report is that the legislation is detrimental in allowing the Agencies to adapt to change. With regards to terrorism this can be extremely devastating as terrorist organisations will continuously adapt and evolve in response to the organisations tasked with combating them. Likewise, cyber is constantly evolving. Unlike terrorism, this is not necessarily as a result of illicit intentions, but simply the nature of it – to be constantly striving for newer and better technology.

Intelligence and Security Act 2017

New Zealand's core intelligence organisations, established during World War II and in the years following this, have grown dramatically since their inception. The governing legislation was shown to need a serious overhaul with the 2009 review of the New Zealand Intelligence Community by Simon Murdoch and the following 2010 Defence White Paper. The Murdoch Report noted that there was a need to clarify the role and responsibilities of the agencies in regard to the 2005 Domestic and External Security Committee of Cabinet 'charter', which set out the integration of the intelligence community. Murdoch noted that it "should identify roles and responsibilities of all those stakeholders in national security who create or consume intelligence[36]". Not having defined roles and

[32] Ibid, p. 7
[33] Ibid
[34] Ibid, pp. 14 - 15
[35] Ibid
[36] Murdoch, S. (12 October 2009). *Report to the State Services Commissioner: Intelligence Agencies Review*, p. 5

responsibilities has proven to be a continuous issue, coming to the forefront very publicly with the Kim Dotcom scandal. Murdoch ends the Report stating that there needs to be an examination of how to "optimise the effectiveness of our intelligence and security arrangements across the New Zealand intelligence community as a whole[37]", and how to maximise the efficiency of the agencies.

Echoing the intelligence situation globally, while there had been some efforts at unifying national intelligence post-September 11, these efforts were merely attempting to build upon the existing intelligence structures and adapt them to the changing world. It was the gradual push showing that these structures were not fit for purpose, being better suited to the Cold War period than being utilised to counter international terrorism and the fluidity of non-State actors. James Whibley notes that the 2010 White Paper "realizes the changing overarching security context: economic weight is shifting, new technology is materializing that narrows several military aspects where New Zealand's traditional partners previously dominated, and non-state actors are able to pose a threat to the state through asymmetric acts[38]".

The report also outlines that as the threat of cyber attacks grow, so too does the potential harm that could be done due to the increasing reliance on web-based networks. Within this there is the risk that if New Zealand does not keep pace with the changes in this area, then "we could become the weak link in the shared effort to deter hostile cyber intrusions … the international community seems poised on the edge of a new and potentially more unpredictable age of proliferation, accentuated by emerging military technologies[39]". Building upon the 2010 Paper, the 2016 Defence White Paper states that "The amount of data stored digitally, and the number of devices connected to each other and the internet, is rising in both the civilian and military context. This increase, alongside the potential for significant disruptions to electronic communication and command and control systems, means cyberspace, and the threat to New Zealand civilian and Defence Force networks from cyber attacks, is growing in importance[40]".

While the Defence White Papers have noted the ever-increasing importance of cyber, and the Murdoch Report outlined that there were some ambiguities in the role and functions of agencies, it the 2013 Kitteridge Report and the subsequent 2016 Report that lead to the Intelligence and Security Act of 2017. The Act brought the existing legislation together under a single, cohesive, unifying Act, which clarified the Agencies' objectives and the scope of their activities, and provided provisions for how they interact with each other (which was one of the issues of confusion with the existing GCSB Act 2003, which did not specify the support that could be provided for other governmental agencies), with Section 13 stating implicitly that it is a function of the intelligence and security agencies to co-operate with each other, and the New Zealand Defence Force and Police. This is one of the pressing issues that Lucas Kello had noted about legislation and cyber: it does not keep pace and is showing no signs of slowing down. The new Act, whilst it may not necessarily be fit for purpose in 20 years, it does resolve and provide clarification around many of the issues that have plagued the intelligence community.

New Zealand Security Intelligence Service

There have been success stories already showcasing how the Intelligence and Security Act 2017 is working in fostering an inter-agency environment, whereby the agencies are supporting one another to achieve outstanding results. The Department of the Prime Minister and Cabinet has declassified several case studies, one of which is prominent in highlighting how the new Act has been a drastic improvement for New Zealand's Intelligence Community by clarifying the use of telecommunications intercepts against New Zealand citizens.

[37] Murdoch, S. (12 October 2009). *Report to the State Services Commissioner: Intelligence Agencies Review*, p. 12

[38] Whibley, J. (2014). One Community, Many Agencies: Administrative Development in New Zealand's Intelligence Services, *Intelligence and National Security, 29*(1), pp. 122-135, p. 122

[39] Ministry of Defence. (17 November 2010). *Defence White Paper 2010*, p. 25

[40] Ministry of Defence. (8 June 2016). *Defence White Paper 2016*, p. 30

The case study details an investigation by the New Zealand Security Intelligence Service investigating a potential Islamic State terrorist. A "trusted foreign liaison partner" has informed the SIS that the suspect, a man known as 'Dave', has been in contact with the Islamic State of Iraq and the Levant and has been living amongst them, is attempting to travel to New Zealand at the behest of the group, and has a New Zealand mobile phone number. To further assess the risk that this could pose, the investigating officer, using 'Dave's' mobile phone number as a reference point, searches NZSIS archives, revealing no information; requests information from other governmental agencies, which uncover 'Dave's' real identity and that he is due to return to New Zealand in just two days' time; then asks for further information from New Zealand's international partners, which show that the facilitator that 'Dave' has been in contact with is an ISIL recruiter.

Further investigation into 'Dave's' closely associated reveals that 'Dave' and the facilitator spend a considerable amount of time talking on the phone, prompting SIS to apply for a Type 1 Intelligence Warrant, to allow the interception of communications of a New Zealand citizen. The warrant is approved, and monitoring of their communications reveal that they have booked one-way flights to Syria for the following week. Confident that 'Dave' is intending to travel to Syria to with the intention of joining the Islamic State of Iraq and the Levant, and may ultimately end up engaging in acts of terrorism, the decision was made to revoke the targets' passport to severely inhibit his ability to travel, and continue to monitor and investigate his activities.

Not only showing how effective the new governing legislation is in action, the case study here also shows the effectiveness of the Intelligence Cycle. The NZSIS had received credible intelligence of a potential threat, and directed an investigation into this. During the course of this investigation a warrant was used to collect additional evidence, which was then collated to make an assessment. Through analysing all the evidence, a report was written which ultimately resulted in action being taken and the cycle beginning again with an further monitoring and investigation.

New Zealand Intelligence Community

The New Zealand Intelligence Community, or NZIC, is primarily composed of three agencies: Government Communications Security Bureau (GCSB), New Zealand Secret Intelligence Service (NZSIS), and National Assessments Bureau (NAB). While other governmental organisations such as the New Zealand Defence Force, New Zealand Customs Service, New Zealand Police, and Immigration New Zealand have intelligence units, the NZIC forms the core of New Zealand intelligence.

Tasked with the protection of New Zealand's national security, international relations and economic well-being of the nation, the NZSIS was officially formed in 1969 with the NZSIS Act. While it had existed since 1956, it was known as the New Zealand Security Service and it had no governing legislation - it was the 1969 Act that defined its role in protecting the State[41].

The agency responsible for providing assessments has been known by a variety of names over the years, including Joint Intelligence Organisation in 1949, Joint Intelligence Bureau in 1953, External Intelligence Bureau in 1975, External Assessments Bureau in 1988, and, since 2010, the National Assessments Bureau (NAB). Becoming a civilian organisation and part of the Department of Prime Minister and Cabinet (DPMC) (having previously been a military department), the National Assessments Bureau is tasked with providing "analysis on events or developments that are relevant to New Zealand's national security and international relations … [utilising] publicly available information such as news media and academic writings, as well as official information such as diplomatic reporting and secret intelligence from New Zealand or abroad[42]".

[41] New Zealand Security Intelligence Service. (2017). *History*, https://www.nzsis.govt.nz/about-us/nzsis-history/

[42] Department of the Prime Minister and Cabinet. (18 October 2018). *Intelligence and Assessments*, https://dpmc.govt.nz/our-business-units/national-security-group/intelligence-and-assessments

Government Communications Security Bureau

The primary functions of the Government Communications Security Bureau are to provide cyber threat detection, disruption and protection of information and networks of national significance; conduct cyber threat analysis; and collect intelligence, primarily foreign, to allow the New Zealand Government to generate informed policy and operational impacts. Since the first publishing of Annual Reports in 2003, there has been a gradual evolution in the content published. Beginning with very functional reports in 2003, these have gradually evolved to provide more information about the role that the GCSB plays, to facilitate an open discussion about the organisation.

The 2003 Annual Report states that the major focus of the GCSB is on the war against terrorism and the enhancement of their technical collection and processing capability skills[43]. Subsequent reports state the major focus of the Bureau is on counter terrorism and regional issues in the South Pacific, in addition to providing intelligence and information systems security support to the New Zealand Defence Force and Ministry of Defence. Of note here is in 2006, where the Centre for Critical Infrastructure Protection (CCIP) conducted an inaugural national Cyber Exercise, contributing to an international effort involving both public and private sectors. In addition, was the establishment of a connection with the International Watch and Warn Network, a network of 15 countries operating as a collaborative portal for cyber threats[44]. This marks an interesting turning point in the reporting of the Agency, with the increased, publicly known, connections with the wider international community on cyber issues and in an attempt at creating a collective defence cyber network.

The National Cyber Security Strategy, first published in June 2011, saw the creation of the National Cyber Security Centre (NCSC) within the GCSB. The Strategy states that the "National Cyber Security Centre will build on existing cyber security and information assurance capabilities to provide enhanced protection of government systems and information against advanced persistent threats[45]". The NCSC is responsible to dealing with the advanced cyber threats that could potentially harm the nations national security or economy.

While 2012 was a difficult year publicly for the GCSB following the controversy arising with Kim Dotcom and allegations of illegal spying, the Annual Report notes that there has been the start of awareness surrounding the threat posed to New Zealand from cyber attacks and efforts to improve public defences here. Additionally, the report notes that:

> "The number of cyber intrusions detected continued to rise over the year and it is clear that, unchecked, cyber intrusions are causing significant national security and economic harm to New Zealand interests. The operational response led by GCSB is focused on assisting designated organisations to build and operate secure IT systems, and to discover, detect and mitigate so-called advanced persistent threats[46]."

Similarly, the major focus for the Bureau in 2013 was on ensuring compliance following the Report by Rebecca Kitteridge, with 2014 seeing the implementation of the Telecommunications (Interception Capability and Security) Act 2013.

One of the biggest responses by the GCSB to the ever-growing threat posed by cyber has been with Project CORTEX. While, out of necessity for operational security, little detailed information about CORTEX has been publicly released, this has been a project that the Bureau is extremely proud of. Beginning in 2014, and completed in 2017, Project CORTEX was designed to counter advanced malware and protect "against theft of intellectual property, loss of customer data, destruction or dissemination of private communications, holding data for ransom and damage to IT networks and

[43] Government Communications Security Bureau. (2003). *Annual Report for the Year Ended 30 June 2003*

[44] Government Communications Security Bureau. (2006). *Annual Report for the Year Ended 30 June 2006*

[45] New Zealand Government. (June 2011). *National Cyber Security Strategy*

[46] Government Communications Security Bureau. (2012). *Annual Report for the Year Ended 30 June 2012*, p.10

services[47]". Even before being fully complete CORTEX was seeming to prove highly effective, preventing, in 2016, an estimated $39.47 million in potential harm.

Additionally, an extremely important part of the GCSB's response to cyber is in the Bureau's commitment to its international partners and in sharing information for the benefit of increasing and improving global security. Through the National Cyber Security Centre, 132 cyber security incidents were reported in the first half of 2015 alone, ranging from ransomware to serious attempts to compromise information systems of national significance. Through this they were able to trace the origins of a new, sophisticated attack to a known threat source and then share the information about this with international partners, promoting vigilance about these attacks and reducing vulnerabilities[48].

The response by the GCSB to cyber has been not merely adapting their traditional role as a communications intelligence agency, but a gradual restructure of the agency with cyber at the forefront. The 2019 Annual Report notes that in December 2018 there were 16 National Security Intelligence Priorities identified. These outline key security issues for New Zealand and include malicious cyber activity and the implications of emerging technology. The latter point here is significant with the Report further stating that "Technological acceleration represents a significant challenge for the GCSB and as new technologies emerge we must be able to react quickly[49]".

New Zealand's Cyber Security Strategy

First published in 2011, *New Zealand's Cyber Security Strategy* lays out how the government is responding to the growing cyber threat, and notes that "The Internet and digital technologies enable New Zealanders to have global access to products and services and reduce our geographical isolation by connecting us with the rest of the world[50]". Such growing connectedness, while helping to promote economic growth, also provides a means of inflicting significant harm. With more than 75% of the nation having access to the Internet in 2009, and with the ever-increasing sophistication of cyber-attacks, the implementation of a cyber security strategy has become a necessity.

The 2011 Strategy states that its purpose is to "raise the cyber security awareness and understanding of individuals and small businesses; improve the level of cyber security across government; and build strategic relationships to improve cyber security for critical national infrastructure and other businesses[51]". The key priority areas here are awareness, protection, and response. By working with organisations such as NetSafe, who provide advice on online safety, the Government can actively pursue dialogue with the general populace about staying safe online and cyber vigilance, and helping people protect themselves and their children from scams, cyber bullying, sexual exploitation, and other cyber issues of increasing prevalence.

The main direct protection and response aspects of the Strategy have been the establishment of the National Cyber Security Centre within the GCSB, and with the establishment of CERTNZ. The National Cyber Security Centre is a part of the Government Communications Security Bureau, providing advanced cyber threat detection and disruption, as well as advice and information on cyber security issues. In addition to CORTEX, other projects undertaken by the NCSC include the Malware Free Networks initiative in 2018, which "involves the NCSC working with internet service providers to deliver 'active disruption' of cyber threats[52]".

[47] Government Communications Security Bureau. (2017). *CORTEX*, https://www.gcsb.govt.nz/our-work/information-assurance/cortex/

[48] Government Communications Security Bureau. (2015). *Annual Report of the Year Ended 30 June 2015*

[49] Government Communications Security Bureau. (2019). *Annual Report of the Year Ended 30 June 2019*

[50] New Zealand Government. (June 2011). *National Cyber Security Strategy*, p. 2

[51] Ibid, p. 6

[52] Government Communications Security Bureau. (21 December 2018). *NCSC Cyber Threat Report 2017/2018*, p. 4

In addition to working with New Zealand Police and CERT NZ domestically, the NCSC also works with a range of international partners, including the Australian Cyber Security Centre, the National Security Agency in the United States of America, the Canadian Centre for Cyber Security, and the National Cyber Security Centre in the United Kingdom. Established in 2016, CERT NZ, or Computer Emergency Response Team, is part of a growing international CERT network, contributing to cyber incident reporting, tracking cyber security attacks, and providing advice on how to respond to and protect against cyber attacks. Working with several key partners, including the Department of Internal Affairs and the National Cyber Security Centre, CERT NZ has five key functions: Threat identification; Vulnerability identification services; Incident Reporting Services; Response Coordination Services; and Readiness Support Services[53].

Comparisons with the 2015 *New Zealand Cyber Security Strategy* help to show some of the effectiveness of the New Zealand Government's response to the cyber threat. Within this it is noted that 90% of households have access to the Internet, and a staggering 83% of people in New Zealand having experienced a cyber breach – up from 70% in the 2011 Strategy report. The 2015 Strategy intends to make New Zealand "a place where: New Zealanders and their businesses prosper; the harm from cyber threats and cybercrime is reduced; fundamental rights online are protected; significant national information infrastructures are defended; and New Zealand is respected internationally as a secure place to do business and store data[54]". This is done through four goals: cyber resilience, cyber capability, addressing cybercrime, and international cooperation.

The 2019 *New Zealand Cyber Security Strategy* notes that within cyber we are rapidly approaching the verge of the next major leap, with the upcoming roll-out of the 5G network and the advent of quantum computing. In his Ministerial Foreword statement, Minister of Broadcasting, Communication and Digital Media Kris Faafoi states that:

> "These new technologies will be disruptive. That will allow us to innovate, but may also expose us to greater risk. These technological changes are not happening in a vacuum: the geopolitical picture has also shifted, with a greater range of state actors making the most of cyber-enabled tools to steal information, spread disinformation and launch attacks. New Zealand's response to the evolving risk needs to be commensurate with our dependence on internet connectivity.[55]"

This is something that the NCSC is also preparing for, stating in their 2017/18 *Cyber Threat Report* that the 5G networks "will place data closer to the end user, using virtualisation technologies rather than having core functions centralised in one location. The spread of these 'core' functions across the network increases the attack surface[56], making it more difficult to protect the confidentiality, availability, and integrity of the data traversing the network[57]".

Intelligence in New Zealand has grown to not only adapt to advances in cyber capabilities but also in how the Agencies will view cyberspace. Cyber has become much more than merely a tool to be used to enhance intelligence operations – it has become a platform through which intelligence operations can take place. In New Zealand, the approach by the GCSB has gone from using cyber to support other operations to focussing on cyber as a platform. As the use of cyber capabilities is growing among those with illicit intentions, so too is the response to protect national interests. With the increase in hostile campaigns such as phishing, there is an increase in social engagement to provide the public with security advice to mitigate the threat posed.

[53] CERT NZ. (n.d.). *About Us*, https://www.cert.govt.nz/about/about-us/

[54] New Zealand Government. (10 December 2015). *New Zealand's Cyber Security Strategy*, p.5

[55] Department of the Prime Minister and Cabinet. (2 July 2019). *New Zealand's Cyber Security Strategy*, p. 3

[56] Attack surface refers to all the points where an actor could gain access to a system. A network with fewer access points is therefore more secure, or theoretically less vulnerable, than a network with multiple data interface points.

[57] Government Communications Security Bureau. (21 December 2018). *NCSC Cyber Threat Report 2017/2018*, p. 7

3. Innovation and Adaptation to Cyberspace in British Intelligence

British intelligence has evolved considerably over the past hundred years. A revolution borne out of necessity, this was facilitated by rapid advances in communications capabilities and the advent of two World Wars in relatively quick succession. Modern British signals intelligence began with the interception of German radio traffic by the cryptanalysts in Room 40 of the Old Admiralty Building during the First World War. In 1914 there was a recognised need in the United Kingdom to protect their official communications, but there were no permanent plans to be implemented, just procedures in the event of war. Likewise, there was very little in the way of a serious effort to decrypt foreign nationals' communications. To this extent, the first signals intelligence victory that the United Kingdom had over the Germans during the First World War "was in fact MO5b (later MI1(b)), an intelligence section in the War Office … This was largely due to the fact that the French, who had years of Signals Intelligence against the Germans, were prepared to share all that they knew[58]."

While Room 40 did not have much early success with foreign signals intelligence, they did contribute in an extremely significant way: in the sorting and classifying of the German communications. They did not have any success in breaking communications until they received a copy of the Magdeburg Code Book, taken from a German Light Cruiser by the Russian Navy. Until this point, their focus on classifying intercepted messages laid the foundation for traffic analysis, producing a different type of analysis by studying how the German forces communicated[59]. As was noted earlier in the Intelligence Cycle section, collation is one of the main fundamentals of the Intelligence Cycle. Eventually becoming the Government Code & Cypher School, before changing into the present-day Government Communications Headquarters, the GCHQ provides for signals intelligence in the United Kingdom and is one of the core British intelligence agencies. Other core agencies include the Secret Intelligence Services, or MI6, which governs foreign intelligence collection; the Security Service, otherwise known as MI5, is their domestic counter-intelligence and security service; and Defence Intelligence, or DI, which is focussed on gathering and analysing military intelligence.

Government Code & Cypher School

In the opening introductory paragraph of his book on the Government Communications Headquarters, Richard Aldritch states that "'GCHQ' is the last great British secret. For more than half a century, Government Communications Headquarters – the successor to the famous wartime code-breaking organisation at Bletchley Park – has been the nation's largest and yet most elusive intelligence service. During all of this period it has commanded more staff than the Security Service (MI5) and the Secret Intelligence Service (SIS) combined and has enjoyed the lion's share of Britain's secret service budget[60]." This 'elusive agency' remained a secret until 1976 when journalist Duncan Campbell published information about its intelligence operations overseas.

Established on November 1, 1919, the Government Code & Cypher School (GC&CS) was initially a peacetime national signals intelligence and communications organisation within the Admiralty. Headed by Alastair Denniston, the GC&CS was responsible for breaking and reading foreign diplomatic encryption systems, solely focussing on this. During the post-First World War period there was no foreseen need to focus on military intelligence – the advent of a second major war was deemed highly unlikely[61]. It was on 15 August 1939, following Hugh Sinclair's purchase of Bletchley Park, that the War Office relocated GC&CS here, where its intelligence processing and code breaking operations expanded greatly. It was here at Bletchley Park that Alan Turing managed to 'break' the German Enigma cypher system, providing intelligence known as 'Ultra'. Possession of such high-

[58] Government Communications Headquarters. (22 February 2019). *The Birth of Signals Intelligence*, https://www.gchq.gov.uk/information/birth-signals-intelligence

[59] Ibid

[60] Aldritch, R. J. (2019). *GCHQ: The Uncensored Story of Britain's Most Secret Intelligence Agency*, Harper Collins. P. 1

[61] Government Communications Headquarters. (11 March 2019). *Alastair Denniston*, https://www.gchq.gov.uk/person/alastair-denniston

grade intelligence proved to be a boon for the British, but it also posed an issue when it came to dissemination, similar to the earlier example helping to draw the United States into the conflict, this time it was attempting to warn Soviet Union about the upcoming German betrayal and invasion.

Although the British were breaking the very weak Soviet cyphers, it seemed highly unlikely that Hitler would engage in fighting across multiple fronts, and the Soviets were not yet involved in the war. Even when they discovered that German units were beginning to mass on the Eastern Front, the concept of invasion did not seem plausible, and certainly not a notion that Soviet dictator Joseph Stalin would ever entertain. Stalin famously rejected any evidence that did not support his beliefs, leading to many intelligence failures in the Soviet Union. Here he believed that any suggestions of war were simply the West seeking to provoke war between Germany and the Soviet Union. Indeed, in June 1941 Germany did invade the Soviet Union.

Bletchley Park began to pursue a loose intelligence alliance with the Soviets, seeking to trade low-grade intelligence. Where Bletchley Park was interested in any intercepted communications, the Soviets tended to view captured documents as being of supreme importance, to the detriment of all else. While the idea of leaving the Soviets and the Germans to fight one another alone filled many in the United Kingdom with joy, it was ultimately decided that to support them in defeating the Nazis was the better option. The issue at hand then was in how to provide the Soviets with information gleaned from Ultra, without letting either side know the true origins of this – the Soviet Union had a tendency to use low-level cyphers for highly classified documents, and if the Germans knew that their Enigma cyphers were broken then they would use new ones. Many Enigma decrypts had discussed the poor cyphers used by the Soviets. The British attempted to warn their ‘allies’, but without being able to provide evidence then such warnings were not acted upon[62].

The issues here around safeguarding capabilities is not something easily resolved and is especially prominent with intelligence sharing agreements. When intelligence is shared and intended to be kept secret, the State is relying on another actor for the security of this. A highly prominent example of this is with the leaking of information to the media by Edward Snowden in 2013. The debates caused as a result of this dominated news media globally for some time and are still making headlines today. Within New Zealand it cast a large spotlight on the GCSB about what capabilities they had for collecting intelligence, and what our involvement with the Five Eyes network was – a spotlight that an intelligence organisation typically tries to stay out of. While whistleblowing and debates around capabilities of an organisation are not unique or limited to cyber, the allegations of mass surveillance, collection of meta data, and accessing of private communications are within the confines of cybersecurity agencies like the GCSB, GCHQ, and NSA.

Government Communications Headquarters

The Government Code & Cypher School officially became known as the Government Communications Headquarters in June 1946, and has grown tremendously since its inception, indeed outgrowing the doughnut-shaped building before construction was complete in 2004. Tasked with counter-terrorism, cyber security, promoting the United Kingdom’s strategic advantage, combating serious and organised crime, and providing support to defence, the GCHQ is the United Kingdom’s principle signals intelligence agency. Having undergone several transformations since its inception, it was during the 1990’s that the Agency was redeveloped into the modern signals intelligence agency it is. Redesigned not just because of the rise of the Internet and developments in modern technology, there was the “realization that what was needed was not just a new technical infrastructure, or even new organogram, but a radically different type of organization. GCHQ had to be able to cope with the fact that virtually all of its targets were now using the same technology, and that techniques developed against one target were likely to be of direct relevance to many others[63]”.

[62] Aldritch, R. J. (2019). *GCHQ: The Uncensored Story of Britain’s Most Secret Intelligence Agency*, Harper Collins.

[63] Pepper, D. (2010). The Business of Sigint: The Role of Modern Management in the Transformation of GCHQ, *Public Policy and Administration, 25(*1), pp. 85-97, p. 88

In May 2016 the GCHQ announced their presence on social media platform Twitter, signalling a shift away from the traditionally secretive and 'hidden' world of intelligence. Adopting social media and adapting to the way in which cyber is being used, helps the agency to recruit from a new generation, and to promote cyber security awareness. Engaging with the general public in a familiar way has also helped the agency to regain and strengthen trust and legitimacy, which may have been negatively affected amidst accusations of mass surveillance, with former Deputy Prime Minister John Prescott tweeting "After years of following us, we can now follow them"[64]. The increased use of social media has proven popular with intelligence agencies internationally and is an interesting way of adapting to cyber. Engaging socially helps the agency to create an image of being open and transparent (as much as a secret agency can be), and also helps them to achieve one of their main goals of ensuring the security of the state by promoting vigilance online in a more effective manner than before.

In additional to adapting to advances in cyber, changes within the organisation have been brought about as a result of terrorist incidents, both within the United Kingdom and elsewhere around the world. On 7 July 2005, at 8:50 am, four suicide bombers attacked London, three of them targeting the underground trains and one, an hour after the initial attack, a bus, killing in total 52 people and wounding more than 700. The most devasting international terrorist attack since 9/11, and indeed in the United Kingdom the worst incident since the Nazi bombings during the Second World War. Following this devastation, there was need for a renewed defence strategy, that was focused on three things: "First, they prioritised front line support to the police and security services … Second, it set a large team to work on 'target discovery', using its databases to try and uncover intelligence on the attacks and all those who might be linked to them. Finally, it created a 'Blue Skies Team' to try and develop new approaches to identify people connected to the bombers[65]."

The idea of 'target discovery' using databases to identify potential extremists is a rather interesting development. After the events of 9/11, agencies had a reinforced emphasis on identifying and tracking terrorist and extremist organisations. When news media reported on communications, such as mobile phone chatter and emails, use among the extremist organisations dropped off significantly for a time. Due to this caution, agencies like the GCHQ used traffic analysis, examining call patterns to identify the various groups. Following this was the use of 'voice prints', "which allowed them [GCHQ] to search volumes of traffic for people who 'sounded like' the suspects. The British were apparently the first to provide an authentic recording of bin Laden's voice, which was then used in this way[66]." The audio recording of his voice was taken from a televised interview on Al Jazeera, and then used to search through the vast database of phone calls recorded via satellite.

Additionally, the GCHQ notes another example of how the use of cyber and advanced communications tracking technologies enabled them to assist MI5 in identifying a person of interest. Within this, an overseas intelligence source informed MI5 that a member of the terrorist organisation ISIL (Islamic State in Iraq and the Levant) leadership handed an envelope to an unknown person, saying that "(the message contained) information for the brothers in the United Kingdom that will cause carnage across London[67]." The information that the source was able to pass onto MI5 about this was that the person of interest here spoke both English and Arabic, had a generic mobile phone, and a high-end tablet. Without additional knowledge, MI5 was unable to pursue this lead further, and requested the GCHQ investigate this further.

[64] Lomas, D., McLoughlin, L., & Ward, S. (2020). 'Hello World': GCHQ, Twitter and social media engagement, *Intelligence and National Security*, *35*(2), pp. 233-251

[65] Aldritch, R. J. (2019). *GCHQ: The Uncensored Story of Britain's Most Secret Intelligence Agency*, Harper Collins. Pp. 501-502

[66] Ibid, pp. 483-484

[67] Government Communications Headquarters. (8 June 2016). *How Does an Analyst Catch a Terrorist*?, https://www.gchq.gov.uk/information/how-does-analyst-catch-terrorist

To identify the person of interest here, they began by looking at the ISIL member, who was known to them, and monitored his communications activity (in this case phone records) around the date of the initial interaction. From this, and with what can be identified and hypothesized about the person of interest, they are able to narrow the search, and identify a pattern of calls that fit the pattern established for this unknown person -that is, that they had been at a specific location, on a particular day and time, and had been in contact with a specified group. With this information helping to narrow the search for this person, they are able to track his communications, and note that he has accessed an online account revealing his name. The person of interests' identity, and their recent online history – which is still in keeping with the extremist profile initially hypothesized – back to MI5 to resume their investigation[68].

One aspect that GCHQ Director Jeremy Fleming has noted is that the GCHQ is becoming a cyber organisation in addition to their role in intelligence and counterterrorism[69]. Director Fleming here notes that:

> "GCHQ's role has always been to collect and use intelligence to disrupt, divert and frustrate our adversaries. We've been doing this since 1919 and we're very good at it … We have a longstanding mission to keep sensitive information and systems secure. This has a distinguished history, notably in protecting our own secrets in wartime. But it too often felt like the poor relations. Our new mandate, to help make the UK the best place to live and do business online, has transformed that perception. This profound development is led within GCHQ by the National Cyber Security Centre … [70]"

Similarly, there have been significant advances in utilising cyber to detect and monitor potential terrorists in Israel, with Managing Director of the Israel Security Agency (ISA), Nadav Argaman, disclosing in to 2017 that by combining data taken from social media platforms with it's own databases, it was able to identify and detain 400 potential terrorists[71]. As Israel has experience a sharp rise in 'lone wolf' terror attacks in recent years, the new tracking system is proving to be a significant boon.

National Cyber Security Strategy

Published in 2016, the National Cyber Security Strategy outlines how the nation is adapting to cyber and the issues that are associated with this. One way in which the United Kingdom is responding to the increased cyber threat is through their Cyber Essentials programme. The scheme helps organisations to protect themselves against low-level threats and "lists five technical controls (access control; boundary firewalls and Internet gateways; malware protection; patch management and secure configuration) that organisations should have in place[72]." With many cyber attacks exploiting basic vulnerabilities such as out out-of-date software, the scheme seeks to help prevent future loss through poor systems management.

The *National Cyber Security Strategy 2016-2021* also notes that in 2016 "the average cost of breaches to large business that had them was £36,500. For small firms the average cost of breaches was £3,100. 65% of large organisations reported they had suffered an information security breach in the past year, and 25% of these experience a breach at least once a month. Nearly seven out of ten attacks involved viruses, spyware or malware that might have been prevented using the Government's Cyber Essentials Scheme[73]."

[68] Ibid
[69] Fleming, J. (17 October 2017). *Protecting the Digital Homeland is Critical to Keeping the UK Safe*, https://www.gchq.gov.uk/news/protecting-the-digital-homeland-is-critical-to-keeping-the-uk-safe
[70] Ibid
[71] Barnea, A. (2018). Challenging the "Lone Wolf" Phenomenon in an Era of Information Overload, *International Journal of Intelligence and Counterintelligence, 31(*2), pp. 217-234
[72] United Kingdom Government. (1 November 2016). *National Cyber Security Strategy 2016-2021,* p. 42
[73] Ibid, p. 42

The Strategy announced plans to transform the United Kingdoms' cyber security capabilities, pledging £1.9 billion towards this. The Strategy notes that "we are critically dependent on the Internet. However, it is inherently insecure and there will always be attempts to exploit weaknesses to launch cyber attacks. This threat cannot be eliminated completely, but the risk can be greatly reduced to a level that allows society to continue to prosper, and benefit from the huge opportunities that digital technology brings[74]." Seeking to mitigate such risks, the Strategy outlines three main focus areas: Defend, Deter, and Develop.

Within the 'Defend' focus area, the Strategy notes that should the United Kingdom maintain their current approach this will not be sufficient in keeping the nation safe from cyber harm. The persistent nature of those who would seek to exploit vulnerabilities or directly attempt to inflict cyber harm means that the United Kingdom must inevitably work harder "to defend the UK against evolving cyber threats, to respond effectively to incidents, to ensure UK networks, data and systems are protected and resilient[75]." One way to help achieve this is thorough Active Cyber Defense (ACD), which "refers to cyber security analysts developing an understanding of the threats to their networks, and then devising and implementing measures to proactively combat, or defend, against those threats[76]." The network being defended here is United Kingdom cyberspace, and actively defending it will ideally help to increase the costs and risks associated with targeting the United Kingdom, reduce the amount of incoming malware, secure communications and internet traffic, and further secure the nations' critical infrastructure. Working with communications service providers, GCHQ, and Ministry of Defence, success here will be measured by the amount of malware and cyber attacks that have been blocked. Without going into detail about how this is happening, the Strategy notes that "the UK is harder to 'phish', because we have large-scale defences against the use of malicious domains, more active anti-phishing protection at scale and it is much harder to use other forms of communication, such as 'vishing' and SMS spoofing … GCHQ, the Armed Forces' and NCA capabilities to respond to serious state-sponsored and criminal threats have significantly increased[77]."

The 'Deter' area is focussed on raising the costs of mounting a cyber attack against the United Kingdom, and in taking serious action once an attack has been made. The Strategy states that "Our adversaries must know that they cannot act with impunity: that we can and will identify them, and that we can act against them, using the most appropriate response from amongst the tools at our disposal. We will continue to build global alliances and promote the application of international law in cyberspace[78]." The terrorist event that transpired on September 11, 2001, saw intelligence budgets around the world drastically increase as counter-terrorism became a pressing issue. In the United Kingdom, the GCHQ had only been monitoring al Qaeda since 2000, picking up increased chatter the following year, but had not been entirely focused on this – while the National Security Agency in the United States of America had been monitoring them more closely following the bombing of American embassies in Kenya and Tanzania in 1998[79]. Counterterrorism has since remained a prominent issue, and with the rise in cyber so there has been a slow rise in terrorist use of the Internet and their cyber capabilities. The Strategy here notes that, while the technical capabilities of terrorists are limited, they will ensure that the threat posed here remains low by committing to detecting and disrupting terrorist activities and threats where these arise in cyberspace. A key way in which the United Kingdom will deter adversaries is through the National Offensive Cyber Programme (NOCP). The programme, developed as a partnership between the Ministry of Defence and the GCHQ, involves "deliberate intrusions into opponents' systems or networks, with the intention of causing damage, disruption or destruction[80]", and has been designed to both add a deterrent element to hostile cyber actors (where

[74] Ibid, p.9

[75] Ibid, p.13

[76] Ibid, p.33

[77] Ibid, p.35

[78] Ibid, p.47

[79] Aldritch, R. J. (2019). *GCHQ: The Uncensored Story of Britain's Most Secret Intelligence Agency*, Harper Collins.

[80] United Kingdom Government. (1 November 2016). *National Cyber Security Strategy 2016-2021*, p.51

the State likely has considerably more resources to counter-attack), and to also complement offensive military action.

Lastly, the ‘Develop’ element looks directly at how the United Kingdom, and through this the Government Communications Headquarters, will respond and adapt to the continued advances in cyber. The develop aspect requires planning not just for the interim five years (which is the scope of the *National Cyber Security Strategy 2016-2021*), but planning for the next twenty years, to ensure that education providers are able to supply efficient cyber security professionals, that the government had certifications and standards in place for this, and that academia will continue to grow within this field. One way in which the United Kingdom is seeking to ‘future-proof’ their cyber capabilities is through horizon scanning, where they are attempting to anticipate what may affect their cyber resilience in five to ten years and building towards this. In doing so they “recognise that horizon scanning goes beyond the technical, to include political, economic, legislative, social and environmental dimensions[81]”.

National Cyber Security Centre

Founded in October 2016, the National Cyber Security Centre (NCSC) is a part of the Government Communications Headquarters, focussing on understanding cyber security and responding to incidents to reduce the harm caused to interests in the United Kingdom, helping to secure both public and private sector networks, and supporting academia and industry providers in building the United Kingdoms’ cyber capabilities. The 2019 NCSC Annual Review notes that they have taken a holistic approach in providing cyber security for individuals by minimising the threat posed to the majority of the population, making it easier to receive cyber security advice, providing tools for the general public to protect themselves, and by raising awareness about cyber security[82]. Noting that in the year ending March 2019, there was an estimated 966,000 computer misuse incidents in the United Kingdom, involving cyber criminals “sending malicious emails, social engineering (the manipulation of people into performing an action or giving away confidential information), water holing (a website infected with malware or containing a link to malware) and by making them download malicious software and apps[83].”

As has been noted before (and was especially apparent during the 2016 US Election Campaign hack), it is the human element that proves the weakest link in cyber security and poses a significant issue for intelligence organisations. In a nation such as the United Kingdom, where there is extensive use of the internet and internet-capable devices, a malicious campaign can pose significant risk to the nations’ economic welfare. Indeed, the human element refer to not just the seeming absence of digital literacy where people fall victim to malicious cyber scams and crime, but also to the failure of analysts to realise the value of intelligence presented to them, or pursue leads where they should have. The suicide bombings that took place in London on 7 July 2005 show an example of the failure of intelligence here. While those involved in the bombings had been influenced by British Muslim websites, they had no direct link to al Qaeda, as initially claimed by British authorities. Indeed the perpetrators had been under surveillance by British intelligence in 2003, but their ties to other extremists were never fully explored and their networks were never mapped out, which may have resulted in the terrorists being arrested before they could carry out their deadly attack[84].

In regard to this, the NCSC has noted that they are looking at ways of redefining how cyber security is viewed by the general populace, and in how people can be secure without feeling restricted. The Report states that:

> “We look at the interaction between people and technology and try to make it easier for people to be secure … One of the most important things we’ve seen is the changing mindset

[81] Ibid, p.61

[82] National Cyber Security Centre. (23 October 2019). *Annual Review 2019*

[83] National Cyber Security Centre. (23 October 2019). *Annual Review 2019*, p. 12

[84] Barnea, A. (2018). Challenging the “Lone Wolf” Phenomenon in an Era of Information Overload, *International Journal of Intelligence and Counterintelligence*, *31*(2), pp. 217-234

> between the idea of ‘let’s alter the behaviour of the person or assume they are going to make a mistake’ to ‘how can we support developers to make more secure and user-friendly products?’ … Instead of forcing security rules on people, we are aiming to make it more approachable through clearer language. To do this, we look towards experts in communications, marketing and advertising, to refresh the message, always with the aim of ensuring the public feel that security is a help, not a hindrance[85].”

In aiding the public to protect themselves online, the NCSC has launched the Cyber Aware campaign, which is a part of a set of initiatives involving a wide array of government departments, industry leaders, and trusted third party actors. In addition to working with manufacturers to ensure the security of software, the NCSC has begun publishing guidelines and small memos. For example, to reduce the number of people falling for scams during Black Friday and Cyber Monday, the NCSC, in consultation with cyber security experts from Microsoft and the British Retail Consortium, published seven tips to help keep people safe. Published on social media, these were ‘shared’ 900 times, ‘liked’ 2,100 times, and increased the amount of people following the NCSC on Twitter to over 50,000.

Additionally, the NCSC had recently launched the Cyber Defence Ecosystem (CDE), which is designed to “Create a structured and automated ecosystem across the UK (and in time globally); Share ‘our part of the puzzle’ to better defend the UK, partners and allies; Build and enhance threat awareness to enable better detection and defence; Rapidly alert enterprise victims of malicious activity[86]”. Designed to complement the Active Cyber Defence programme, the CDE is not just to share knowledge, but to create a shared database to allow faster and better response to incidents, and to allow organisations to respond to their own incidents thus freeing up valuable resources for use elsewhere.

The response here by the NCSC is interesting in that it is both a response to the changing nature of societies relationship with cyber and indicative of the changing persona of intelligence organisations. Cyber has penetrated almost all aspects of society, with a significant majority of people in developed nations being constantly connected to digital media via the Internet. The response here by the NCSC has been to embrace and adapt to the meteoric rise of social media by actively asking people to monitor them so they can receive updates and information promoting cyber security and staying safe online. Additionally, it is indicative of the changes in British intelligence (and elsewhere in the world) by actively acknowledging the existence of organisation and their activities (as noted earlier, the existence of the GCHQ was considered a national secret), and by encouraging discussion of cyber security and what is happening globally, with the increased public cyber attacks by state and non-state actors, in an effort to actually promote national security.

[85] National Cyber Security Centre. (23 October 2019). *Annual Review 2019*, p. 12

[86] Ibid, p. 47

3. United States of America

Signals intelligence in the United States of America has grown tremendously since the start of the 20th century, in both size and scale and in organisational 'maturity'. During the Second World War signals intelligence in the US was extremely fragmented, agencies in competition with one another, and with the Army and Navy both having strong signals intelligence and cryptanalytic abilities but operating completely independent of each other. It was not until the end of the Second World War that there was a push towards inter-agency cooperation and for intelligence to be governed by its own separate Agency. It was in 1944 that was there were the beginnings of inter-agency cooperation, with the establishment of the Army-Navy Communication Intelligence Coordinating Committee (ANCICC), a forum for discussing cryptologic issues. This eventually became the Army-Navy Communication Intelligence Board (ANCIB), a civilian agency that was accepted by the Department of State. Here the Army agreed to monitor communications from military radio stations and military messages, with the Navy handling their counterparts. This left the issue of coverage of diplomatic targets. A viable long-term solution was not found at this stage, with several efforts attempted such as the Army decrypting on odd days of the month and the Navy on even days. This proved decidedly to not be feasible.

It was in June 1942 that an agreement was reached, stating that responsibility for military traffic and diplomatic communications lay with the Army, and the Navy was "responsibility for enemy naval traffic, enemy naval air and weather systems, and through its wartime control of the Coast Guard, surveillance of clandestine communications … The FBI, in addition to sharing the responsibility with the Navy for clandestine targets in the Western Hemisphere, worked domestic voice broadcasts and domestic criminal actions[87]". Burns further states that "The wartime agreements had accomplished little more than a basic division of labor and had avoided the real issue of establishing a centralized cooperative effort. In the main, the spirit of the earlier measures seemed to reflect an inherent attitude that cooperation in COMINT matters was a necessary evil, rather than any real conviction about the benefits of centralization or cooperation. Seeking to shelter their vital COMINT functions from further budget reductions, the military authorities intensified their efforts to achieve closer cooperation and coordination between their COMINT organizations[88]". Here, the differing groups – the U.S. Army, Navy – can be seen as regarding cooperation as a necessary evil, something that they have to work around in order to, at the very least, maintain their current budget, or gain an increase if they can attain further control of COMINT functions.

Additional agreements between the military forces soon followed. Whilst throughout the war the Army and Navy had maintained separate relations with the United Kingdom, Aldritch notes here that "In 1953 the British approached the Americans to suggest a combined organisation for planning electronic warfare and radio countermeasures … the two nations managed to get together for a major US/UK Electronic Warfare Conference every two years … it was becoming harder to distinguish between signals that carried communications and other types of electronic signals[89]". Prior to this, the United States and the United Kingdom had initiated the discussion culminating in the British-United States of America Agreement (BRUSA), which "was predicated in part on the existence of centralized controls of COMINT activities within both countries, the approaching ratification and implementation of the agreement brought a new, compelling urgency for the United States to put its own house in order[90]". The BRUSA agreement was a forerunner to the present-day AUSCANNZUKUS Agreement, better known as 'Five Eyes'.

[87] Burns, T. L. (1990). *The Origins of the National Security Agency 1940-1950 (U)*, Centre for Cryptologic History, p. 12

[88] Ibid, p. 30

[89] Aldritch, R. J. (2019). *GCHQ: The Uncensored Story of Britain's Most Secret Intelligence Agency*, Harper Collins. P. 116

[90] Burns, T. L. (1990). *The Origins of the National Security Agency 1940-1950 (U)*, Centre for Cryptologic History, p. 35

Changing priorities in the post-war period led to the focus here being redirected towards the Soviet Union, and in turn generated an increased need for a single agency, where "The end of World War II signalled the beginning of the end of the exclusive military domination of the Army and Navy COMINT organizations. Because of the increased emphasis given to economic, political, and diplomatic intelligence, civilian agencies now pressed for a much greater voice in the direction of U.S. COMINT activities[91]". Furthermore, as the BRUSA Agreement depended upon COMINT being centralised, the current fragmented situation within the United States would not be enough to meet the demands here.

The United States' intelligence history, leading up to the creation of the National Security Agency, is interesting in how markedly different it is compared to other nations. The NSA was born out of necessity, not just to address the growing communications intelligence sector, but because the alternative arrangement, having it continue to be segmented among the military with support from civilian agencies like the F.B.I, was so inefficient and wrought with internal politicking that there was no other option but a complete restructure. After several failed early attempts at creating a centralised communications intelligence service, including the establishment of the Armed Forces Security Agency (which failed as it did not actually centralise COMINT), and the administering of cryptographic functions by the newly created Air Force Security Service. The Army argued for a single, unified SIGINT organisation, like that adopted by the British, stressing "the need for consolidating into a single armed forces activity all but the most narrowly defined problems of primary interest to each service[92]". When the SIGINT and COMSEC functions of the Army, Navy, and Air Force were combined, the Air Force and, to some extent, the Army found loopholes to avoid cooperation and undermine the efforts of others. The outbreak of the Korean War in 1950 placed a renewed pressure on the need for well organised intelligence services, exposing some of the limitations of the 'unified' effort. With mounting displeasure and frustrations with the timeliness and quality of the intelligence output, and critiques by civilian organisations like the C.I.A, the National Security Agency was formally introduced on October 24, 1952, by President Harry Truman.

National Security Agency

Whilst the National Security Agency is not the only organisation in the United States of America focused on Signals Intelligence, it is the most prominent and is the equivalent of the New Zealand Government Security Communications Service and the United Kingdoms' Government Communications Headquarters. Founded in 1952, the National Security Agency (NSA) has since become the largest intelligence organisation in the United States of America. Tasked with signals intelligence and cybersecurity, the NSA has noted that the newest and fastest growing threat to national and economic security are those developing in cyberspace. While cyberspace and the use of the Internet allows the States to grow significantly, as noted earlier it is inherently insecure and comes with many vulnerabilities.

Initially tasked with monitoring and analysing traffic on radio waves, the advent of networked computing marked a significant turning point in the NSA, and brought about a jurisdictional battle with the CIA. Interagency conflict, something not unfamiliar in the United States, and indeed not something unique to the State, eventually gave way to the realisation that co-operation tends to yield more efficient results. The advancement of cyber and its rapidly expanding use, particularly from the early 1990's onwards, brought about an organisational evolution in the NSA, ensuring their continued focus on "activities designed to study and collect how signals and data are communicated and what can be divined from those communications … Given that signals analysis and development along with other technical intelligence subfields rests on technological trends, there exists a disposition to continually be aware of technologies, communication systems, and how these trends impact mission

[91] Ibid, p. 27
[92] Ibid, p. 64

requirements[93].” From this, the evolution was natural, with the Agency adapting to remain relevant in a world with rapidly advancing and changing means of communication.

One aspect of cyber that has proven to be an issue for the NSA, and other agencies internationally, is that they are increasing unable to target individual communication networks. During the Cold War, for example, they were able to target individual, isolated communication networks and means of communication utilised by Soviet agents. As there has been the widespread advent of public communication networks interlinked digitally, it is simply no longer enough to target the individual network. A prime example here is with the rise of Al Qaeda, who will utilise these public networks, and ‘hide in plain sight’, to organise and relay messages among themselves with a greatly reduced risk of detection – targeting communication from an individual agent may yield results, but simply targeting the means of communication may no longer be practical[94].

In 2013 Edward Snowden made news headlines globally by revealing that he was employed as a contractor with the NSA to conduct mass surveillance and that, through the use of sophisticated computer software, could wiretap anyone anywhere in the world and monitor everything that they did online. All that he needed to do this was their personal email address. These allegations drew widespread international condemnation and sparked a number of intelligence and security reviews. These allegations also named the United Kingdom, Canada, Australia, and New Zealand as being complicit through their involvement in the ‘Five Eyes’ intelligence sharing involvement.

Foreign Intelligence Surveillance Act 1978

For almost 100 years the United States of America has conducted some form of electronic intelligence gathering, aiding in the disruption of subversive foreign actors, the arrest of lawbreakers and capturing of terrorists, in addition to providing valuable foreign intelligence. Such abilities and powers, however, must by democratic necessity be used only for legitimate purposes and targeting those necessary for achieving the required outcome, i.e. not used for nefarious purposes, such as spying on a domestic political rival.

It was a Supreme Court decision in 1972 requiring the use of a warrant or judicial sanction for intelligence to be collected against U.S. citizens, following the United States’ Senate investigation into the gross misuse of power and illegal covert operations domestically by the FBI and CIA that led to the Foreign Intelligence Surveillance Act (FISA) being adopted in 1978. The Act also established the FISA Court, which provides “judicial oversight to the gathering of foreign intelligence for national security purposes[95]”. The oversight here is of supreme importance, with Judge Gorton noting further that “Before there was a FISA Court, one agency of the Executive could decide when another agency of the Executive was entitled to conduct electronic surveillance and physical searches for that purpose[96]”.

Boykin notes that, where the Act allowed for surveillance of foreign powers or their agents, “A United States person could not be regarded as a foreign power for purposes of obtaining an order from the FISA Court for activities protected by the First Amendment. Nevertheless, a United States person could be an agent of a foreign power when the person engages in clandestine intelligence activities on a foreign power’s behalf, when such activities may involve a violation of the criminal laws of the United States[97]“.

[93] Loleski, S. (2019). From Cold to Cyber Warriors: The Origins and Expansion of NSA’s Tailored Access Operations (TAO) to Shadow Brokers, *Intelligence and National Security*, *34(*1), pp. 112-128, p. 116

[94] Ibid

[95] Gorton, N. M. (2014). Reflections of a Former FISA Judge, *Boston Bar Journal*, *58*(2), p. 1

[96] Gorton, N. M. (2014). Reflections of a Former FISA Judge, *Boston Bar Journal*, *58*(2), p. 1

[97] Boykin, S. A. (2016). The Foreign Intelligence Surveillance Act and the Separation of Powers, *University of Arkansas at Little Rock Law Review*, *38*(1), pp. 33-62, p. 37

It was after the events of September 11, 2001, that the USA PATRIOT Act (formally known as the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act) was adopted. Enacted with little opposition, the Act held a number of significant provisions, including "Enhanced surveillance procedures for law enforcement, including amendments to the Foreign Intelligence Surveillance Act (FISA). Specifically, the Patriot Act gave federal officials new surveillance authority in terrorism cases, as well as the ability to conduct searches of property without the consent or knowledge of the owner or occupant[98]". Furthermore, Section 206 of the USA PATRIOT Act enables for the issuing of a roving warrant, where investigators can use the single FISA warrant to track a target regardless of whether they change communication devices – previously a FISA warrant would be targeting a single device, meaning agents would need to obtain a separate warrant for each device used.

The 2004 Intelligence Reform and Terrorism Prevention Act (IRTPA) also allowed for FISA warrants to be issued against 'lone wolf' agents – those who would meet requirements for a FISA warrant except for having no explicit ties with a foreign power or terrorist organisation[99]. This provision greatly expanded the scope with which FISA warrants could be issued, such as for non-terrorism related cyber crime. While he was on the FISA Court from 2001 to 2008, serving before the recent controversies began, Judge Gorton ends his reflections by stating that:

> "The Foreign Intelligence Surveillance Act was designed to (and does, in fact) provide for the protection of civil liberties, and the judges of the FISA Court diligently see to it that the statue is enforced … I am disturbed by the recent rash of condemnation of the work of the National Security Agency and the effort to curtail significantly its surveillance function. The work of law enforcement officers involved in our national security that I witnessed, and temporarily joined in overseeing, saves lives; and their investigations do not unduly invade the privacy of U.S. citizens. The FISA Court plays a vital and necessary role in that regard, a role that should be acknowledged and protected by our leaders[100]."

9/11 and the 'War on Terror'

On September 11, 2001, 19 hijackers took control of four commercial airplanes. American Airlines Flight 11, with 92 people on board, was flown the North Tower of the World Trade Centre in New York at 8:46 am; United Airlines Flight 175, with 65 people on board, was flown into the South Tower of the World Trade Centre at 9:03 am; American Airlines Flight 77, with 64 people on board, was flown into the side of the Pentagon at 9:37 am. Lastly, United Airlines Flight 93, with 44 people on board in total, crashed into a field near Pennsylvania at 10:03, shortly after passengers had retaken control of the aircraft. What has become known as the darkest day in American history, and indeed the most devastating terrorist attack to date, killed 2,977 people, and sparked the US-led 'War on Terror'. One major impact that this had is in the revolutions in American intelligence.

Chomik notes that "The security landscape was rapidly changing due to the amorphous nature of unconventional non-state threats such as al-Qaeda and the Taliban, along with their increasing ability to use technology for nefarious means … The USIC needed methods to become more responsive and to transform into a more cohesive unit of cooperating agencies that shared resources, rather than 16 different silos operating independently of each other[101]". It was this, the failure of agencies to cooperate with one another and to share intelligence, that was cited as one of the reasons that 9/11 was able to happen – agencies had intelligence that this was possible, but no sharing or discussion meant it was completely overlooked.

[98] Peritz, A. J. & Rosenbach, E. (2009). *Confrontation or Collaboration? Congress and the Intelligence Community*, Belfer Center for Science and International Affairs, p. 2

[99] Ibid

[100] Gorton, N. M. (2014). Reflections of a Former FISA Judge, *Boston Bar Journal*, *58*(2), p. 2

[101] Chomik, A. (2011). Making Friends in Dark Shadows: An Examination of the Use of Social Computing Strategy Within the United States Intelligence Community Since 9/11, *Global Media Journal – Canadian Edition*, *4(*2), pp. 95-113, p. 98

As discussed above, the USA PATRIOT Act 2001 was an extremely important response to this, providing provisions for increasing and expanding the scope within which surveillance powers can be utilised by intelligence agencies. Critically, this removed the provision that agencies are only able to conduct surveillance against those considered an ‘agent of a foreign power’, i.e. not a US citizen.

One other important introduction to the US intelligence community was the ‘Intellipedia’, a “community-wide, crowd-sourced wiki used to build a database of information that is only accessible within the USIC and across secure internal networks[102]”, allowing analysts from different agencies to share information, connect socially, and collaborate in cyberspace. One of the dangers of increased inter-agency visibility and sharing is the increased risk of information leaking out and privacy breaches, such as was the case with Bradley Manning, who stole hundreds of thousands of documents, which were subsequently published on WikiLeaks, leading to “public embarrassment on the part of the U.S. government and left questions about the ease of accessibility into otherwise secure networks used in the USIC, such as SIPRNet or the Joint Worldwide Intelligence Communications Systems (JWICS)[103]”. The actions of just one person can have a significant impact on severely damaging the trust between agencies, undermine the public faith in the State, and potentially jeopardise ongoing operations or even compromise the safety and security of intelligence agents, highlighting the need for effective internal oversight and monitoring of compliance.

It is important to note that the response by the US to the terrorist attacks is significant as it did bring about greatly increased inter-agency cooperation as they worked towards a unified goal. Further to this, the shifting focus for intelligence and the legislative enactments provided significant resources for adapting to cyber. The Agencies were able to track a target with a single FISA warrant, were more focused on monitoring communications and, where possible, disrupting terrorist communication networks and their ability to communicate effectively.

Offensive Capabilities

In early 2010 centrifuges in Iranian nuclear facilities were able to enrich uranium from 3 percent to 20 percent, signalling a major step in the ability to manufacturer nuclear weapons (90 percent is considered bomb-grade uranium). An alternative to targeted missile strikes against the facilities, a computer virus was employed to inhibit Iran’s ability to enrich uranium. Developed by the United States and Israel, the virus, known as Stuxnet, exploited several zero-day vulnerabilities in Microsoft software to cause the centrifuges to spin increasingly faster and tear themselves apart. Destroying almost 1,000 centrifuges and slowing down Iran’s ability to refine uranium, the virus showed the very real effect that a well-executed cyber attack can have[104].

Of particular note is how the United States, among other nations, are developing offensive cyber abilities, and how these weapons differ from conventional means of attack. With conventional armaments, having more advanced tools can typically sway the odds in your favour – such as with the introduction of automatic rifles and body armour. With cyber, however, the significant factor resulting in success or failure is in the skills and abilities of the operatives – the ‘cyber warriors’. It is the skill and experience of the cyber warriors, and their ability to react and adapt in real-time, that often determines the outcome of a cyber operation. The ability to control the outcome of a cyber operation is extremely important as cyberweapons typically tend to become obsolete after their initial use. This is because once used it is possible for the opposing party to determine how the attack was able to compromise their systems and then fix the vulnerability. In this regard knowledge of vulnerabilities and exploits is a particularly valuable commodity for intelligence agencies[105]. Slayton here cites a Defense Science Board task force as stating that most “successful attacks reaching DoD [Department

[102] Ibid, p. 99
[103] Ibid, p. 106
[104] Freedman, R. (2011). Stuxnet’s Impact, *Baltimore Jewish Times, 318*(4), pp. 34-37
[105] Slayton, R. (2017). What is the Cyber Offense-Defense Balance?: Conceptions, Causes, and Assessment, *International* Security, *41(*3), pp. 72-109

of Defense] networks today result from a personnel failure or out-of-date software in firewalls and detection systems. Most of these attacks are understood and preventable through known signature management (patching), yet DoD defense systems don't keep up, and attacks continue to penetrate DoD's networks[106]".

Cyber weapons that exploit vulnerabilities in software are also particularly susceptible to obsolescence before that may be used. A weapon may be rendered ineffective if the software is patched, and the vulnerability no longer exists. As software is generally in a constant state of being updated and patched (at least, with good systems administration anyway), there can be time constraints imposed on the development of a cyber weapon. One concept driving the offense in the US is that of 'persistent engagement', the main doctrine being pushed by NSA director and Commander of US Cyber Command Army Gen. Paul Nakasone. The aggressive strategy involves tracking targets and taking offensive cyber action against them – something that will help further deter potential cyber assailant by establishing the US as a dominant cyber actor capable of targeted, direct action. Anne Neuberger, head of the newly formed Cybersecurity Directorate, has stated persistent engagement is "Knowing that we're not waiting for the incident, we're tracking, we're understanding, we're degrading their capabilities, their ability to operate in a way that hopefully prevents that key attack[107]".

[106] Ibid, p. 87

[107] Myre, G. (26 August 2019). *'Persistent Engagement': The Phrase Driving a More Assertive U.S. Spy Agency*, https://www.npr.org/2019/08/26/747248636/persistent-engagement-the-phrase-driving-a-more-assertive-u-s-spy-agency?t=1583919442321

5. Issues Posed to Intelligence by Cyber

Taking a somewhat collaborative approach to cyber has not always been the direction undertaken by intelligence agencies, and it does not specifically address several key issues posed by cyber. One of the main issues is with legislation. Agencies are typically restricted in what they can do because of the wording of the relevant legislation, something which is a significant issue with cyber. The nature of cyber involves it constantly evolving and improving, seemingly without limitations. Legislation enacted in the early 2000's does not provide provisions for communications intelligence derived from social media – social media was not relevant at this point, not beyond forums or message boards. One issue that this had posed was in that agencies were unsure what their legal standing was here. Rapid advances in cyber tend to create grey areas because there has been no precedent set.

The above three national case studies have shown some of the approaches to cyber that have been taken, showing that it is the States' recent history that has greatly impacted on their intelligence reforms – in New Zealand a significant factor was in clarifying the legislation in light of recent controversies and allowing them to operate more efficiently in cyberspace. In the United Kingdom we have seen tremendous increases in social engagement with the public in response to the rapid rise in hostile cyber campaigns. And in the United States of America, the response to 9/11 has seen greatly increased funding for their intelligence agencies and amendments to legislation allowing for increased surveillance against persons in the State.

Whilst such responses may be a boon to their respective intelligence agencies, they are not without their issues. The following section will discuss three of these issues: the Tallinn Manual as an attempt to engage with international law and how this may impact intelligence agencies; the right to privacy and the approaches to this that have been taken by Australia, Russia, the United Kingdom, the United States of America, and Germany; and lastly, the use of cryptography and the ongoing efforts by States at undermining the private use of this.

Tallinn Manual

There have been several attempts at engaging international law about cyber, which has resulted in publications such as the Tallinn Manual. While not legally binding, the Manual provides an analysis on how existing international law can be applied to cyberspace, noting that "The Tallinn Manual 2.0 analysis rests on the understanding that the pre-cyber era international law applies to cyber operations, both conducted by and directed against states. This means that cyber events do not occur in a legal vacuum and states both have rights and bear obligations under international law[108]." A key issue with this passage, however, is that to take action against a state for hostile cyber activities then they would need to prove that it was the state that conducted such hostilities – and not, for example, a non-state actor. Tracing the origins of cyber activities can be extremely difficult. The Tallinn Manual takes into account several aspects of cyber to construct its discussion, such as where a cyber-attack may cause bodily damage, harm to life, or destruction of property, and that it has cross-border elements making international law applicable. Additionally, where we can draw distinctions between land, sea, and air, and the States' sovereignty over this, we may also draw such distinctions with cyberspace, and that where a computer in one state is used to attack a computer in another state, this may be considered an international armed attack, under certain conditions[109].

It is important to note that the Tallinn Manual is not to be taken a best-practice guide, but rather an examination of how international law could be applied to cyber phenomena. A fitting example of this is with sovereignty, where under international law an intentional violation of a States' sovereignty is a wrongful act, this could apply to cyber where "an agent of one State uses a USB flash drive to introduce malware into cyber infrastructure in another State, a violation of sovereignty has taken

[108] The NATO Cooperative Cyber Defence Centre of Excellence. (2020). *Tallinn Manual 2.0*, https://ccdcoe.org/research/tallinn-manual/

[109] Efrony, D. & Shany, Y. (2018). A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice, *The American Society of International Law*, *112*(4), pp. 583-657

place[110]". With the above example, there are critics of this who argue that this should not be seen as a violation of sovereignty, and cyber operations should be considered instead international espionage. This is not prohibited under international law, and "espionage may violate international law only when the modalities employed otherwise constitute a violation of a specific provision of international law, such as unlawful intervention or use of force[111]". In this regard it is argued further that cyberspace should not be considered a sovereign domain, as sea, air and land are. Sovereignty and cyber is an interesting discussion as there is no universally accepted notion of what this is.

Furthermore, there is the question of attribution for cyber-attacks. Margulies notes that "The *Manual* relies on the International Law Commission's *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, which tie state responsibility to showing that a private party is 'acting on the instructions of, or under the direction or control of' a state[112]", reinforced by the International Criminal Tribunal for the Former Yugoslavia that "held that state officials may be accountable if they exercised 'overall control' over a group or entity[113]." Merely providing financial and technical resources would not satisfy this, however[114]. For a State to be able to retaliate here, the scale of the cyber-attack would need to be comparable with a physical, armed attack, to avoid escalating the situation further into armed conflict.

A significant issue here for intelligence agencies is to be able to trace the source of the cyber-attack to attribute it to a State (or non-State entity), and also determine the effects of the intrusion, which in turn may decide any appropriate action to be taken. Margulies further notes that "Cyber is relatively easy to direct, given a sophisticated commander, but very difficult to detect … unlike convention kinetic action where effects are manifest within a short time after the weapon is used, cyber-weapons can take months to detect, lying formant for significant periods or secretly altering data to clandestinely compromise a network's operation[115]."

The Tallinn Manual is important moving forward with cyber as it is one of the first major attempts at addressing how international law can be utilised in cyber space. While the Manual is not a legal handbook or guide for cyber, it is an analysis providing a platform for future discussion and legal codification. In this regard it is important for the future of cyber, particularly as hostile cyber actions are increasing in number and with non-state actors accounting for a disproportionate amount.

Right to Privacy

Related to this is the right to privacy, especially with social media. In nations like the United States of America, the United Kingdom, New Zealand, Canada, etc., there are typically provisions in domestic legislation which will outline the rights of citizens and permanent residents to be have freedom of movement and expression and a right to privacy. In this regard, arbitrary surveillance of its people is forbidden, and should only be done so with a warrant showing that there is a valid cause and reason. Programs such as PRISM, which collects metadata indiscriminately, have generate much controversy and media attention internationally as they violate these rights, greatly infringing on privacy and collecting data of people who would otherwise be free from surveillance. Proponents of such programs have advocated the necessity of this, advising that only data directly related to legitimate purposes, such as the prevention of terrorism by allowing agencies to quickly map communication data, will be accessed – irrelevant data will be destroyed in a given time frame.

[110] Jensen, E. (2017). The Tallinn Manual 2.0: Highlights and Insights, *Georgetown Journal of International Law*, *48*(3), pp. 735-778, p. 741

[111] Schmitt, M. N. (2017). Respect for Sovereignty in Cyberspace, *Texas Law Review*, *95*(7), pp. 1639-1670, p. 1643

[112] Margulies, P. (2013). Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility, *Melbourne Journal of International Law*, *14(*2), pp. 496-519, pp. 497-498

[113] Ibid, p. 498

[114] And likewise, actions taken by a private person could not be attributable to the State, under international law.

[115] Margulies, P. (2013). Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility, *Melbourne Journal of International Law*, *14(*2), pp. 496-519, p. 500

Eliza Watt notes that “Article 17 ICCPR and Article 8 ECHR apply extraterritorially, which means that states must respect the right to privacy whenever individuals are within their territory as well as their jurisdiction[116]”, with the United States stated that they have no obligations toward respecting and protecting such rights outside their territories. Debates around the right to privacy, and the wider protection of individual human rights, and cyber is ongoing, with further controversial legislation being passed by States internationally.

Australia has recently passed the Telecommunications (Assistance and Access) Act 2018, which compels companies to provide assistance to government agencies and undermine encryption by allowing access to messages and files. The Act has been highly controversial and reminiscent of a police state. While Australia already had legislation requiring communications providers to supply agencies with a target’s communications where requested, there were concerns that illicit actors were utilising the end-to-end encryption offered by communications applications like WhatsApp to deny the agencies access. The Bill, which was rushed through Parliament with little opportunity for discussion, states that it “equips agencies with the tools they need to effectively operate in the digital era … the measures enhance the existing ability of Australian agencies to undertake targeted, proportionate and independently oversighted surveillance activities[117]”.

While the Australian Department of Home Affairs have stated that they are unable to compel an industry to break encryption, there are fears that this could require providers to create a ‘back-door’, which will allow the agencies access when presented with a warrant. As it is not possible to create such access targeting just one person, any move updating the software would affect all users, undermining the security of the application and their users’ right to privacy[118]. Furthermore, in 2018 Russia banned the use of Telegram, an encrypted messaging application, due to its refusal to cooperate with Russian intelligence services. Russian authorities had requested that the messaging service allow the State to read the encrypted messages that users domestically were sending and receiving[119]. The request here builds upon the 2016 anti-terrorism law reforms, known as the ‘Yarovaya law’, which “obliges telephone and internet providers to store records of all communications for six months and all metadata for three years, as well as help intelligence agencies decode encrypted messaging services[120]”.

Within the United States and the United Kingdom there have been controversy over the use of cyber intelligence programs such as Stingray, which track and monitors mobile phone connections; MUSCULAR, which obtains data from internal Yahoo! and Google networks; and TREASUREMAP, a highly ambitious programme designed to provide a global map of the Internet, showing in real time what is being accessed from any connected device. XKeyscore and PRISM have also gained immense media attention since their existence was revealed by former NSA contractor Edward Snowden. Developed by the NSA, XKeyscore allows an analyst to search, using only a targets email address, “through vast databases containing emails, online chats and browsing histories of millions of individuals[121]”. Der Spiegel also announced in 2013 that XKeyscore was being used by German foreign intelligence agency BND, and that they had been working very closely with the NSA in

[116] Watt, E. (2017). The Right to Privacy and the Future of Mass Surveillance, *The International Journal of Human Rights, 21(*7), pp. 773-399, p. 776

[117] Department of Home Affairs. (16 September 2019). *The Assistance and Access Act 2018*, https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/data-encryption

[118] BBC World News. (7 December 2018). *Australia data encryption laws explained*, https://www.bbc.com/news/world-australia-46463029

[119] MacFarquhar, N. (13 April 2018). *Russian Court Bans Telegram App After 18-Minute Hearing*, The New York Times, https://www.nytimes.com/2018/04/13/world/europe/russia-telegram-encryption.html

[120] Luhn, A. (26 June 2016). *Russia Passes ‘Big Brother’ anti-terror laws*, The Guardian, https://www.theguardian.com/world/2016/jun/26/russia-passes-big-brother-anti-terror-laws

[121] Greenwald, G. (31 July 2013). *XKeyscore: NSA tool collects ‘nearly everything a user does on the internet’*, The Guardian, https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data

intelligence sharing[122]. Advanced surveillance technologies like those outlined above gives rise to the concept of global surveillance, where surveillance has "developed from a practice carried out manually into something now undertaken on a global scale and largely operated by machines[123]" using algorithms to locate individuals who digital footprint may indicate illicit intent.

Much of the discussion regarding the individual right to privacy as competing with the need for ensuring State security is centred around the issue of terrorism. In 2013, for example, France's then-technical director of the *direction générale de la sécurité extérieure* (DGSE), stated, in response to their collection of telecommunications metadata, "Today, our targets are the networks of the public at large, because they are used by terrorists[124]".

In Germany, in 2016, it came to light that the Federal Intelligence Service, or BND, was only able to monitor 10 messaging services, out of 70 in use, due to end-to-end encryption, something which severely impacted upon the data that could be collected. To this end, the "BND requested an extra €73m in 2017, to set up project Panos, which would work to find weaknesses in messenger apps to circumvent end-to-end encryption … the agency requested additional funding to buy expertise from external companies and service providers to help decrypt data and to break devices[125]." Surveillance by the State is not something that has suddenly been made possible with the advent of cyber – it has been happening for thousands of years and is a necessity for the survival of the State. By spying on targets (both foreign and domestic) the State is able to, amongst other things, keep apprised of threats and take action accordingly. What cyber and the 'digital revolution' alter is the scale with which the State can spy. Intelligence agencies are now able to monitor and map internet traffic globally, using the information to identify potential criminal networks and hostile actors (both foreign and domestic), and track malicious cyber actors. The greatly enhanced cyber abilities, however, come with a trade-off – the loss of privacy for everyone. Cyber does not discriminate, and the internet is a truly global phenomenon, meaning that agencies around the world can, and will, engage in mass surveillance – the only real restriction inhibiting a States' ability to do so is the skill of their cyber operatives.

Cryptography

As noted previously, encryption was a big issue for Kim Dotcom and Megaupload. Previously there had been the so-called 'Crypto Wars' involving, notably in the United States of America, attempts by government to prevent public use of military grade encryption software, thereby making it easier for intelligence agencies to break into civilian encryption domestically. There were efforts during the 1990's to inhibit and restrict the development and sale of commercially available encryption, with governments fearing that strong encryption would be propagated by those with illicit intent, such as paedophiles, the criminal underworld, enemies of the State and foreign agents. If they could ensure that weaker encryption was utilised, then it would be easier for government agents, like the NSA, to break, and therefore supposedly strengthening national security. In short, these 'Crypto Wars' were lost, and there has been relatively free development and dispersion of high-end encryption.

Bruce Schneier, a leading cryptographer, cyber security specialist, and fellow at the Berkman Center for Internet & Society at Harvard Law School, stated that "The government lost the crypto-wars … Crypto is now freely available but in a sense they won because there are so many ways at people's data that bypass the cryptography. What we're learning from the Snowden documents is not that the NSA and GCHQ can break cryptography but that they can very often render it irrelevant … They

[122] Der Spiegel. (20 July 2013). *German Intelligence Used NSA Spy Program*, https://www.spiegel.de/international/germany/german-intelligence-agencies-used-nsa-spying-program-a-912173.html

[123] Petit, P. (2019). 'Everywhere Surveillance': Global Surveillance Regimes as Techno-Securitization, *Science as Culture*, *29(*1), pp. 30-56, p. 31

[124] Anderson, N. (7 June 2013). *France Also Scoops Up Phone, Internet Metadata On Its Citizens*, arstechnica.com, https://arstechnica.com/tech-policy/2013/07/france-also-scoops-up-phone-internet-metadata-on-its-citizens/?comments=1&post=24846805

[125] Soesanto, S. (2018). *No Middle Ground: Moving On From The Crypto Wars*, European Council on Foreign Relations, p. 24

exploit bad implementations, bugs in hardware and software, default keys, weak keys, or they go in and break systems and steal data[126].”

In 2016 there was a case within the US where James Comey, as then-Director of the FBI, engaged in a legal battle with Apple, in a failed attempt to force the company to write firmware to unlock an iPhone 5C. Apple’s refusal to cooperate led the FBI to contracting Cellebrite, an Israeli mobile forensics company, to bypass the iPhone’s security, at a cost of USD $900,000[127]. The inability to bypass commercial encryption has had a significant impact on law enforcement, with Christopher Wray, the successor of James Comey as Director of the FBI, to note that in 2017 alone the Bureau was “unable to access data from 7,775[128] encrypted devices … despite possessing legal permission to obtain the information. The consequences of going dark on these devices has … resulted in major setbacks in a number of cases related to counter-terrorism, human trafficking, and organised crime[129]”.

There has also been a very recent case emerge detailing the CIA and West-German intelligence secretly owning and running a prominent cryptography corporation providing ‘secure’ devices to States and corporations for more than 50 years. Since the end of the Second World War the United States and Germany have jointly owned and operated cryptographic devices manufacturer Crypto AG, a Swiss-based company who sold devices to more than 120 countries. The highly classified operation allowed the United States and Germany to easily read messages sent by Iran, the Vatican, India, and Pakistan, to name a few. It has been noted that, from 1970 onwards, “the CIA and its code-breaking sibling, the National Security Agency, controlled nearly every aspect of Crypto’s operations … They monitored Iran’s mullahs during the 1979 hostage crisis, fed intelligence about Argentina’s military to Britain during the Falklands War, tracked the assassination campaigns of South American dictators and caught Libyan officials congratulating themselves on the 1986 bombing of a Berlin disco[130]”. Accurately fearing the closeness of the company with the West, Russia and China were never clients of Crypto AG, but intelligence operators still learnt a lot about the two States from what other States were saying about them.

Additionally, the NSA has been accused by former contractor Edward Snowden of intentionally infecting commercial products, granting them remote access. Involving prominent companies like “Western Digital Corp., Seagate Technology Plc., Toshiba Corp., IBM, Micron Technology Inc., and Samsung Electronics Co Ltd. … since at least 2010 the NSA has routinely received or intercepted routers, servers, and other networking equipment being exported from the US to foreign customers … The agency, allegedly, obtains the package, implants their backdoor tools, then repackages the devices with a factory seal and forwards them to the customer. The infected devices eventually connect back to the NSA[131].” Very similar to the warnings against using Huawei technology, it seems that the NSA may have been doing the very same thing.

Similarly, within the United Kingdom one programme undertaken by the GCHQ is Tempora, which taps into the transatlantic fibre cables provided by major telecommunications companies to monitor and decrypt internet traffic. The effectiveness of Tempora, however, is mitigated by the increased use

[126] Corera, G. (16 March 2014). *Who is winning the ‘crypto-war’?*, BBC World News, https://www.bbc.com/news/magazine-26581130

[127] Soesanto, S. (2018). *No Middle Ground: Moving On From The Crypto Wars*, European Council on Foreign Relations

[128] The information Wray cited for this figure came from several databases, causing the same devices to be counted multiple time. The actual number of devices the FBI was unable to access was about 1,000 – 2,000.

[129] Soesanto, S. (2018). *No Middle Ground: Moving On From The Crypto Wars*, European Council on Foreign Relations, p. 11.

[130] Miller, G. (13 February 2020). *German/US spies owned encryption company used by allies and adversaries*, stuff.co.nz, https://i.stuff.co.nz/world/americas/119462712/germanus-spies-owned-encryption-company-used-by-allies-and-adversaries

[131] Medina, R. & Pulver, A. (2018). A review of security and privacy concerns in digital intelligence collection, *Intelligence and National Security, 33*(2), pp. 242-243

of personal encryption technologies employed by the general populace. In this regard, it could be seen as being in the interests of the GCHQ to discourage the use of sophisticated encryption technology, enabling them continued access to internet traffic flow[132]. While it may be argued that allowing the GCHQ access to unencrypted internet traffic is necessary for national security purposes, it is important to emphasise that their ability to monitor this, that is the lack of widespread use of encryption, does not discriminate.

[132] Ibid, p. 242

6. The Huawei Scandal

On December 1, 2018, Canadian authorities arrested Meng Wanzhou, Huawei's chief financial officer and daughter of the companies' founder and CEO Ren Zhengfei, over allegations of theft of trade secrets in the United States of America. Reaching this culmination after more than six years of growing mistrust and accusations of spying for the Chinese government, the arrest made headlines globally. The accusations initially began in December 2001, with Indian intelligence accusing Huawei of aiding Taliban forces in Afghanistan by supplying them with communications equipment. Both Huawei and China denied such allegations, and without further proof or details of the technology supplied, it was thought that the accusations may have been politically motivated as a result of China's close military ties with Pakistan[133]. The first allegation of intellectual property theft arose in January 2003 with Cisco filing a lawsuit against Huawei, claiming that they stole source code, documentation, copyrighted materials and other patents[134]. Huawei admitted that it had used some Cisco code, but that this was accidental and that the offending code has since been removed[135]. The lawsuit was then settled out of court in 2004, with provisions for an independent review of Huawei's technology to verify that it no longer contained intellectual property belonging to Cisco[136].

Following this was a warning in 2009 by the GCHQ to BT (formerly British Telecom) that technology supplied by Huawei could "be hijacked by China to cripple the UK's communications infrastructure[137]." Unlike their counterparts in the United States of America, who believed that due to the close relationship that Huawei has with the Chinese military their (Huawei's) systems are compromised, the British deemed the risk of this is relatively low, but because of the considerably high impact that it would have should it be true then action should be taken. In this instance the recommendation that it gave BT was to not use Huawei for the multi-billion-pound network upgrade. As the BT network is used by military, intelligence, and governmental departments in the United Kingdom, the risk of being compromised, even if the risk is low, is too high to gamble on.

Australia appear to have heeded this advice when, in 2012, they advised Huawei to not submit a tender for their National Broadband Network project, citing security concerns. In addition to the news not being well received by the Chinese company, former Australian Foreign Minister Alexander Downer stated that "the whole concept of Huawei being involved in cyber-warfare is based on the company being Chinese (which is) ridiculous[138]". It would indeed be unreasonable to claim that Huawei should not be trusted imply because they are a Chinese company. However, due to their close ties with the Chinese military, theft of intellectual property (whether intentional or not is difficult to determine, but this was not an isolated issue), where there is doubt, or even a possibility that Huawei's systems are compromised by the Chinese government, then it would not be unreasonable to take mitigating action here. In October 2012, a US congressional panel warned that Huawei posed a security threat, and the CIA claimed that the company is spying for the Chinese government – which was denied by Huawei in July 2013.

Overtaking Apple as the world's send-largest manufacturer of smartphones in 2018, Australia and New Zealand, in August and November 2018, respectively, announced their decision to exclude the

[133] Krishnadas, K. (12 December 2001). *Chinese Telecom Company Accused of Aiding Taliban*, eetimes.com, https://www.eetimes.com/document.asp?doc_id=1144221

[134] Duffy, J. (29 January 2003). *Cisco Sues Huawei Over Intellectual Property*, networkworld.com, https://www.networkworld.com/article/2339527/cisco-sues-huawei-over-intellectual-property.html

[135] Charny, B. (26 March 2003). *Huawei Admits to a Little Copying*, cnet.com, https://www.cnet.com/news/huawei-admits-to-a-little-copying/

[136] The Wall Street Journal (29 July 2004). *Cisco, Huawei Settle Lawsuit*, http://www.wsj.com/articles/SB10910232814167631

[137] Williams, C. (30 March 2009). *Spy Chiefs Warn Over Huawei Gear in 21CN*, theregister.co.uk, http://www.theregister.co.uk/2009/03/30/huawei_threat/

[138] Chirgwin, R. (25 March 2012). *Huawei Banned from Australia's NBN: reports*, theregister.co.uk, https://www.theregister.co.uk/2012/03/25/huawei_nbn_ban/

company from the upcoming 5g network[139]. The Huawei scandal is indicative of a new set of challenges laid before intelligence organisations. Companies are increasingly generating and storing more and more data about their users, and in the case of a smartphone company this can literally be data about its users' entire life – their financial history, full records of all their communications, travel patterns, etc. The allegation that the Chinese government has access to this information, and indeed that the system was designed this way, poses issues for intelligence agencies globally.

[139] BBC World News. (1 November 2019). *Timeline: What's going on with Huawei*, https://www.bbc.com/news/technology-46483337

7. How the US Election Hack Shows the Threat to the State

One of the biggest threats to the State comes not from criminals seeking to exploit the naivety of the general populace or terrorist and extremists attempting to spread messages of hate and recruit vulnerable youths, but from foreign state actors influencing internal affairs and undermining democratic processes. Within the United States a prominent example of this, and to further highlight the bureaucratic divisiveness of the State, is in the 2016 US Election Hack.

Beginning on 19 March 2016, John Podesta, the then-Chairman of Secretary Hillary Clinton's presidential campaign, received an email stating that due to security concerns he had to change his password by following a link in the email. Seemingly innocuous, he followed procedure, nonetheless, forwarding the email to his cybersecurity team to verify its authenticity before proceeding. While the email was illegitimate, a typo in their response saw him informed that the email was legitimate, causing him to use the link in the email to change his password. The email here proved to be a successful spearphishing attempt by Russian-based hackers to gain access to DNC systems. The information gained from this, which included internal assessments of other Presidential candidates including Bernie Sanders and now-US President Donald Trump in addition to private emails, were provided to WikiLeaks who subsequently released the documents. While the Republican National Committee servers were also hacked, none of the information gained here was released, leading many observers to note that the hack here was designed to discredit Secretary Clinton and thereby increase the chances of Donald Trump's campaign. Clinton supports this assertion claiming that Putin has held a grudge against her "since 2011 for inciting mass protests against his regime in late 2011 and early 2012[140]."

While the FBI had first noticed security breaches in the Democratic National Committee (DNC) servers, the DNC's IT department disagreed with the risk posed so concerns were not escalated[141]. It is difficult to say here whether escalating or sharing the FBI's concerns would have made a difference as Podesta's actions were correct in seeking a professional opinion on the email. From this it does appear that the hack began because of incompetence by the DNC's IT department. Again, issues of fragmentation here confound the abilities of the United States to take direct action, as the responsibility for maintaining and ensuring the integrity of voting systems is under the jurisdiction of the individual States. The federal government is left knowing that there are significant issues, but powerless to compel the State to act.

A recent report by the RAND Corporation notes that actors utilising hostile social manipulation may "employ targeted social media campaigns, sophisticated forgeries, cyberbullying and harassment of individuals, distribution of rumours and conspiracy theories, and other tools and approaches to cause damage to the target state[142] ". One thing to be taken from the report is in the question of how does an intelligence agency respond to the hostile use of 'soft' tactics, that is disinformation and social media campaigns directed at the general public? It notes that "Moscow has developed an emerging suite of tools that give it the potential ability to have significant, perhaps even decisive impacts on electoral outcomes[143]", which was apparent during the US Presidential Election. While they may be able to take some action to remove social media pages publishing 'fake news', they are highly limited in what they can do without violating the right to freedom of speech and expression, and, as with terrorism, it is extremely difficult to remove all the inflammatory content – people are still able to access articles spreading disinformation.

[140] Office of the Director of National Intelligence. (January 6 2017). *Assessing Russian Activities and Intentions in Recent US Elections*. National Intelligence Council, p.1

[141] Sciutto, J. (28 June 2017*). How One Typo Helped Let Russian Hackers In*. CNN, https://edition.cnn.com/2017/06/27/politics/russia-dnc-hacking-csr/index.html

[142] Beauchamp-Mustafaga, N., Casey, A., Demus, A., Harold, S. W., Matthews, L. J, Mazarr, M. J., & Sladden, J. (2019). *Hostile Social Manipulation: Present Realities and Emerging Trends*, RAND Corporation, p. ix

[143] Ibid, p. xi

Where cyber has increasingly become concerned with use by the general public, so has the response from intelligence agencies become more focused on their interplay with the public, and in promoting a much more cooperative relationship. There has also been evidence emerge showing Russian and Venezuelan involvement in influencing the issue of Catalan independence in Spain, and Chinese social media has also been sharing such propaganda material. In 2017 alone, of the more than 5 million messages on social media about this, more than 97 percent came from accounts originating in Russia and Venezuela. Through this it has been noted that States traditionally hostile to the West, such as Russia, China, Venezuela, Iran, and North Korea, could "work together in creating alternative information systems, promoting counter-narratives, and achieving specific disruptive effects[144]." Blurring the lines even further within cyber between what is real and what is fiction could ultimately result in "the deep fragmentation of global information networks, including the internet itself, into competing and mutually exclusive zones, with profound effects on world politics and international relations. This process is already well underway with the efforts on the part of several countries, most notably China, to build what amount to parallel internets[145]." Already there have been some early attempts at fragmentation of the internet, with the recent internet neutrality discussions.

The 2016 US election hack is particularly interesting as it serves to highlight the difficulties that government agencies have in taking action to protect civilian agencies. The FBI had brought the intrusions into the DNC servers to the attention of their (the DNC's) IT team in 2015, but this was not followed up on. Similarly, NSA website notes that:

> "Our information networks and technology are constantly at risk from a variety of bad actors using a multitude of techniques – remote hacking intrusions, the placement of malware, spearphishing and other means of gaining access to networks and information. Some of these bad actors are criminals motivated by profit … But cyber threats also come from nation states and other actors who seek to exploit information to gain an advantage over the United States … Terrorists and extremist groups today use the power of the Internet, especially social media, to spread their messages of hate and intolerance, and to recruit new members … The global reach of cyberspace and the complexity of its networks provide back actors ample places to hide, safe from the reach of international law[146]."

[144] Ibid, p.167
[145] Ibid, p.167
[146] National Security Agency. (n.d.). *Understanding the Threat*, https://www.nsa.gov/what-we-do/understanding-the-threat/

8. Analysis

Intelligence has grown and changed drastically over the last hundred years, from decrypting communications during the First and Second World Wars to the masses of aerial photography during the Vietnam War, through to modern interconnected technologies. As technology has developed and improved over the years, so too has the response by intelligence agencies, adapting to increased risks and newer threats. Signals intelligence agencies have undergone an immense transformation, from the humble beginnings a hundred years ago, having denied their very existence for decades, to not only acknowledging their secret use by Government but encouraging public participation and involvement to keep the nation safe – no longer the concept of the 'Gentleman Spy'.

Rapid developments in technology, allowing individuals, groups, organisations, and States to connect and interact digitally has revolutionised the way in which we, as a species, communicate. Our entry into the digital era marks a turning point in history, and the implications of cyber are still not yet fully known. The legal system is still trying to adapt, and policymakers are struggling to keep up with the fluidity of the evolution of this period. Where this new digital era is still largely in its infancy, one question it raises is how are intelligence organisations adapting to cyber? We've seen the rise of 'hacktivism', and socially disruptive groups like Anonymous; state-sponsored hacking and the influencing of electoral campaigns; attempts at fragmenting cyberspace; and mass surveillance over an entire population. Cyber is immeasurably immense, essentially forming a new dimension, and through the analysis of publicly released annual reports and academic articles we can see how intelligence agencies around the world are adapting to cyber.

Governments around the world are increasingly adopting a more interconnected social response to the growing cyber threat. The social response is only one part of this, but by engaging with the public this can help the Agencies to become more accepted when it comes to otherwise unpleasant issues, such as a loss of privacy – either actual or perceived. The response by intelligence agencies around the world can be seen as a modern implementation of deterrence policy – ensuring awareness of cybersecurity and current security issues, and education about how people can keep themselves and their businesses secure, helps to further deny, or greatly reduce the effectiveness of, a cyber-attack. Kello notes further here that there is also a self-imposed deterrence, where "the attacker decides not to attack because he believes that the negative consequences will affect him as well[147]". Simultaneously, retaliation for a cyber-attack can be extremely difficult to quantify. One response posed by NATO has been that they could respond to cyber-attacks against member states with direct military action. The issue here is with proportionality, and in how could you measure the impact of a cyber-attack within a reasonable timeframe to justify military intervention? Furthermore, there is also the issue of attribution, in determining not only where a cyber-attack has come from, but also in determining if this was originating from the State, a state-sponsored actor, or a lone-wolf?

We can use the realist political theory to help explain the response by intelligence agencies to cyber globally. Classical realism, as described by Patrick Porter, "begins in pessimism from acknowledgement of the reality of power and the enduring insecurity of the world … It sees systemic pressures as constraining but indeterminate; recognises the force of ideas and domestic politics in driving state behaviour; and treats politics as uncertain, contingent, and subject to the will of agents[148]". The cyber security and the intelligence community field one fraught with insecurity and dubious intelligence, making it, as Porter states, a situation in which governments have no choice but to proceed, where the "difficulty lies in the misplaced confidence in one's own knowledge, the failure to scrutinise assumptions being made, and the failure to insure against the unpredictability of one's own actions and their consequences[149]".

[147] Kello, L. (2017). *The Virtual Weapon and International Order*, Yale University Press, p. 201

[148] Porter, P. (2016). Taking Uncertainty Seriously: Classical Realism and National Security, *European Journal of International Security*, *1(*2), pp. 239-260, p. 251

[149] Ibid, p. 251

Within the Intelligence Cycle, cyber has had a number of impacts, with one of the main points being that the focus of intelligence agencies has typically shifted from using cyber and digital technologies as a tool to becoming the focus of several agencies – i.e. investigating and tracking cyber crime and cyber terrorism, events happening within cyber. One of the other key adaptations to cyber by intelligence agencies has been with changes in public engagement from the agencies to promote and enhance the security of the State. No longer staying 'in the shadows', agencies are acknowledging their existence and reporting on the role they play in ensuring security. Providing a platform for public engagement allows them to effectively promote cyber safety and awareness, reducing the effectiveness of phishing schemes and online scams, thereby protecting the economic interests and security of the State.

In New Zealand two key reports, the Review of Compliance at the Government Communications Security Bureau and Intelligence and Security in a Free Society, helped to enact a legislation reform resulting in the Intelligence and Security Act 2017. Allowing the Agencies to operate much more effectively in the modern era, the GCSB has grown tremendously over the past decade, with the focus of the Agency shifting to be responding to cyber rather than utilising it to achieve other objectives. Similarly, the United Kingdom has also introduced new legislation modernising their intelligence agencies and introduced a Cyber Security Centre. One of the main ways that the United Kingdom has adapted to cyber has been, in addition to increased social media campaigns, the use of 'target discovery', using audio recordings and voice imprints to track targets and rapidly search through existing databases. Intense inter-agency conflict plagued the US, greatly fragmenting the intelligence community, and something which is slowly being overcome with increased shared databases and internal social media. One of the biggest impacts cyber has had in the US has been the legislation changes granting agencies additional powers post-9/11. FISA warrants were now able to cover all means of communication, rather than for one communication device at a time, and the USAPATRIOT Act was introduced, granting sweeping surveillance powers. Furthermore, there has been the significant expansion of offensive cyber abilities. Able to act as a means of deterrence also, development of offensive cyber abilities in the United States forms a significant part of the doctrine of 'persistent engagement', of tracking and engaging targeting and disrupting their abilities to react.

Such developments in cyber have generated significant controversy, however, as outlined in the Tallinn Manual, the right to privacy, and cryptography. The Tallinn Manual represents a significant effort to engage international law with cyber. While not legally binding or to be considered a 'best practice guide', the Manual is an important step in furthering discussion on cyber. With the powers that intelligence agencies have and the ease of cyber in surveillance, there has been significant discussions on the individuals' right to privacy. The powers granted to States by legislative reforms allowing for increased surveillance measures – both domestic and externally – have proven to be a significant boon, allowing authorities to prevent major crime from happening and monitor persons of interests in ongoing investigations. The revelations of Edward Snowden and other whistle-blowers, revealing the existence and use of mass surveillance technologies by the State have brought about renewed discussions of the right to privacy. Whilst surveillance is not something that is new because of surveillance, it is the sheer scale upon which it can be conducted that is the cause for concern, seemingly reminiscent to that orchestrated by Joseph Stalin.

The view that the public use of high-end encryption poses an issue for intelligence agencies as, while they may have the legal authority to access the encrypted information, they lack the ability to do so, is valid. However, the issue of whether there should be restrictions on the availability of high-end encryption, for the purposes of national security, raises several other highly important issues. Cyber does not discriminate, and where insecure, or not-as-secure-as-they-could-be, cyphers are utilised, this reduces the users' ability to be secure from everyone. It is not just agents with he legal authority to access the encrypted information that have an increased chance of doing so, it is everyone with the technical ability. Through this, cyber has had a tremendous impact on intelligence agencies internationally, providing a strong case for legislative changes allowing the Agencies to operate in the modern era and also greatly expanding and developing the surveillance powers of the State. The legitimate causes for enhancing these intrusive powers have generated significant controversy, sparking debates around the legalities of this and the individuals’ right to privacy, issues which are still ongoing with no resolution in sight.

Conclusion

The response by intelligence agencies around the world has been promoting awareness of cybersecurity and current security issues, and education about keeping themselves secure, which in turn helps to further deny or greatly reduce the effectiveness of a cyber-attack.

Much of the discussion in this thesis has been focused on New Zealand, the United Kingdom, and the United States of America to provide an overview of how Western intelligence agencies are adapting to cyber. Other than where they have been discussed in case studies, Russia and China have not been assessed in-depth as there is not enough reliable information about their Agencies, and historically internal politicking has been quite volatile, making the cases in the United States seem like schoolyard squabbles.

Furthermore, whilst these three States, together with Australia and Canada, make up the ‘Five Eyes’ intelligence sharing arrangement, it is also important to take into consideration that on top of this the States may have multiple arrangements and agreements with other States, such as that between the United States and Germany. It was recently revealed that these two States’ intelligence agencies, the CIA and West German intelligence, had covertly owned and operated Crypto AG, a Swiss based firm that manufactured encryption devices. Unbeknownst to the public, these devices were geared to allow access by German and American intelligence forces, enabling them to spy on clients, including the Vatican, India and Pakistan, Iran, and military juntas in Latin America.

The cyber awareness campaigns are designed to increase security from the bottom rungs, to help prevent people from falling victim to various scams and malicious cyber attacks. Whilst this is designed to help prevent significant economic losses to the State, there are also protracted efforts at undermining high-end commercial encryption to allow the State to break and access users’ protected files. Where this is done under the guise of counter-terrorism, when non-Western states, like Russia and China, have adopted these policies they are quickly derided as enacting ‘Big Brother’ laws, before pursuing the same thing themselves, such as in Australia.

There was a similar situation again with the United States and West German intelligence covertly owning and operating a manufacturer of cryptographic devices, within which they had back door access, and then denouncing Huawei for their close ties with the Chinese government. Whilst the scepticism about Huawei devices is well-founded, there is a great deal of fear and hypocrisy between States internationally.

Moving forward one of the main issues yet to be solved will be around attribution and proportionality with cyber attacks. As the Tallinn Manual has identified, it can be very difficult to define what is or is not a violation of a States’ sovereignty, and with the rise in state-sponsored cyber crime it can be difficult to where a cyber attack may have originated from and by whom. The ICTY set a precedent for holding the State accountable for crimes committed by groups that they exercise control over, but often with cyber attacks the difficulty lies in being able to prove who was responsible for this.

Bibliography

Aldritch, R. J. (2019). *GCHQ: The Uncensored Story of Britain's Most Secret Intelligence Agency*, Harper Collins.

Anderson, N. (7 June 2013). *France Also Scoops Up Phone, Internet Metadata On Its Citizens*, arstechnica.com, https://arstechnica.com/tech-policy/2013/07/france-also-scoops-up-phone-internet-metadata-on-its-citizens/?comments=1&post=24846805

Anton, C. (2015). Intelligence Cycle Planning in Military Coalition Operations, *Journal of Defense Resources Management, 6*(1), pp. 133-136

Barnea, A. (2018). Challenging the "Lone Wolf" Phenomenon in an Era of Information Overload, *International Journal of Intelligence and Counterintelligence, 31(*2), pp. 217-234

BBC World News. (7 December 2018). *Australia data encryption laws explained*, https://www.bbc.com/news/world-australia-46463029

BBC World News. (1 November 2019). *Timeline: What's going on with Huawei*, https://www.bbc.com/news/technology-46483337

Beauchamp-Mustafaga, N., Casey, A., Demus, A., Harold, S. W., Matthews, L. J, Mazarr, M. J., & Sladden, J. (2019). *Hostile Social Manipulation: Present Realities and Emerging Trends*, RAND Corporation, p.ix

Boykin, S. A. (2016). The Foreign Intelligence Surveillance Act and the Separation of Powers, *University of Arkansas at Little Rock Law Review, 38*(1), pp. 33-62

Burns, T. L. (1990). *The Origins of the National Security Agency 1940-1950 (U)*, Centre for Cryptologic History

Cambridge University Press. (2019). Intelligence, https://dictionary.cambridge.org/dictionary/english/intelligence

CERT NZ. (n.d.). *About Us*, https://www.cert.govt.nz/about/about-us/

Charny, B. (26 March 2003). *Huawei Admits to a Little Copying*, cnet.com, https://www.cnet.com/news/huawei-admits-to-a-little-copying/

Chirgwin, R. (25 March 2012). *Huawei Banned from Australia's NBN: reports*, theregister.co.uk, https://www.theregister.co.uk/2012/03/25/huawei_nbn_ban/

Chomik, A. (2011). Making Friends in Dark Shadows: An Examination of the Use of Social Computing Strategy Within the United States Intelligence Community Since 9/11, *Global Media Journal – Canadian Edition*, *4(*2), pp. 95-113

Corera, G. (16 March 2014). *Who is winning the 'crypto-war'?*, BBC World News, https://www.bbc.com/news/magazine-26581130

Cullen, M. & Reddy, P. (29 February 2016). *Intelligence and Security in a Free Society: Report of the First Independent Review of Intelligence and Security in New Zealand*

Efrony, D. & Shany, Y. (2018). A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice, *The American Society of International Law*, *112*(4), pp. 583-657

Fleming, J. (17 October 2017). *Protecting the Digital Homeland is Critical to Keeping the UK Safe*, https://www.gchq.gov.uk/news/protecting-the-digital-homeland-is-critical-to-keeping-the-uk-safe

Freedman, R. (2011). Stuxnet's Impact, *Baltimore Jewish Times, 318*(4), pp. 34-37

Government Communications Headquarters. (8 June 2016). *How Does an Analyst Catch a Terrorist*?, https://www.gchq.gov.uk/information/how-does-analyst-catch-terrorist

Government Communications Headquarters (25 January 2019) *Real World Impacts: How GCHQ's predecessors contributed to the US entering World War I*, https://www.gchq.gov.uk/information/century-how-work-gchqs-predecessors-contributed-us-entering-world-war-i

Government Communications Headquarters (22 February 2019) *The Birth of Signals Intelligence*, https://www.gchq.gov.uk/information/birth-signals-intelligence

Government Communications Headquarters (11 March 2019) *Alastair Denniston*, https://www.gchq.gov.uk/person/alastair-denniston

Government Communications Security Bureau. (2003). *Annual Report for the Year Ended 30 June 2003*

Government Communications Security Bureau. (2006). *Annual Report for the Year Ended 30 June 2006*

Government Communications Security Bureau. (2012). *Annual Report for the Year Ended 30 June 2012*

Government Communications Security Bureau. (2015). *Annual Report of the Year Ended 30 June 2015*

Government Communications Security Bureau. (2017). *CORTEX*, https://www.gcsb.govt.nz/our-work/information-assurance/cortex/

Government Communications Security Bureau. (2018). *Annual Report for the Year Ended 30 June 2018*

Government Communications Security Bureau. (21 December 2018). *NCSC Cyber Threat Report 2017/2018*

Government Communications Security Bureau. (2019). *Annual Report of the Year Ended 30 June 2019*

Der Spiegel. (20 July 2013). *German Intelligence Used NSA Spy Program*, https://www.spiegel.de/international/germany/german-intelligence-agencies-used-nsa-spying-program-a-912173.html

Department of Home Affairs. (16 September 2019). *The Assistance and Access Act 2018*, https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/data-encryption

Department of the Prime Minister and Cabinet (18 October 2018) *Intelligence and Assessments*, https://dpmc.govt.nz/our-business-units/national-security-group/intelligence-and-assessments

Department of the Prime Minister and Cabinet. (2 July 2019). *New Zealand's Cyber Security Strategy*

Duffy, J. (29 January 2003). *Cisco Sues Huawei Over Intellectual Property*, networkworld.com, https://www.networkworld.com/article/2339527/cisco-sues-huawei-over-intellectual-property.html

Gorton, N. M. (2014). Reflections of a Former FISA Judge, *Boston Bar Journal*, *58*(2)

Greenwald, G. (31 July 2013). *XKeyscore: NSA tool collects 'nearly everything a user does on the internet'*, The Guardian, https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data

Hastings, M. (2015). *The Secret War: Spies, Codes and Guerrillas 1939-1945*, William Collins.

Hughes-Wilson, J. (2016). *On Intelligence: The History of Espionage and the Secret World*, Constable

Hurley, B. (13 October 2019). *Police build case against 'bumbling Jihadi' Mark Taylor, but outdated anti-terrorism laws could see him walk free*, https://www.stuff.co.nz/national/116471644/police-build-case-against-bumbling-jihadi-mark-taylor-but-outdated-antiterrorism-laws-could-see-him-walk-free

Jensen, E. (2017). The Tallinn Manual 2.0: Highlights and Insights, *Georgetown Journal of International Law*, *48*(3), pp. 735-778

Johnson, L. (2011). National Security Intelligence in the United States: A Performance Checklist, *Intelligence and National Security, 26*(5), pp. 607-615, p. 611

Keegan, J. (2003). *Intelligence in War: Knowledge of the Enemy from Napoleon to Al-Qaeda*, Penguin Random House.

Kello, L. (2013). The Meaning of the Cyber Revolution: Perils to Theory and Statecraft, *International Security*, *38*(2), pp.7-40

Kello, L. (2017). *The Virtual Weapon and International Order*, Yale University Press

Kitteridge, R. (March 2013). *Review of Compliance at the Government Communications Security Bureau*

Krishnadas, K. (12 December 2001). *Chinese Telecom Company Accused of Aiding Taliban*, eetimes.com, https://www.eetimes.com/document.asp?doc_id=1144221

Lomas, D., McLoughlin, L., & Ward, S. (2020). 'Hello World': GCHQ, Twitter and social media engagement, *Intelligence and National Security, 35*(2), pp. 233-251

Loleski, S. (2019). From Cold to Cyber Warriors: The Origins and Expansion of NSA's Tailored Access Operations (TAO) to Shadow Brokers, *Intelligence and National Security*, *34(*1), pp. 112-128

Luhn, A. (26 June 2016). *Russia Passes 'Big Brother' anti-terror laws*, The Guardian, https://www.theguardian.com/world/2016/jun/26/russia-passes-big-brother-anti-terror-laws

Lynch, A., McGarrity, N., & Williams, G. (19 February 2015) Australia's Response to 9/11 Was More Damaging to Freedom Than Any Other Country's, The Guardian, https://www.theguardian.com/commentisfree/2015/feb/19/australias-response-to-911-was-more-damaging-to-freedom-than-any-other-countrys

MacFarquhar, N. (13 April 2018). *Russian Court Bans Telegram App After 18-Minute Hearing*, The New York Times, https://www.nytimes.com/2018/04/13/world/europe/russia-telegram-encryption.html

MacLeod, I. (16 January 2015). Canada's Post 9/11 Anti-Terror Laws, Ottawa Citizen, https://ottawacitizen.com/news/national/canadas-post-911-anti-terror-laws

Malone, R. (2015). Protective Intelligence: Applying the Intelligence Cycle Model to Threat Assessment, *Journal of Threat Assessment and Management*, *2*(1), pp. 53-62

Margulies, P. (2013). Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility, *Melbourne Journal of International Law*, *14(*2), pp. 496-519

Medina, R. & Pulver, A. (2018). A review of security and privacy concerns in digital intelligence collection, *Intelligence and National Security*, *33*(2), pp. 242-243

Miller, G. (13 February 2020). *German/US spies owned encryption company used by allies and adversaries*, stuff.co.nz, https://i.stuff.co.nz/world/americas/119462712/germanus-spies-owned-encryption-company-used-by-allies-and-adversaries

Ministry of Defence (17 November 2010) *Defence White Paper 2010*

Ministry of Defence (8 June 2016) *Defence White Paper 2016*

Ministry of Foreign Affairs and Trade. (2019). *International Security*, https://www.mfat.govt.nz/en/peace-rights-and-security/international-security/

Murdoch, S. (12 October 2009) *Report to the State Services Commissioner: Intelligence Agencies Review*

Myre, G. (26 August 2019). *'Persistent Engagement': The Phrase Driving a More Assertive U.S. Spy Agency*, https://www.npr.org/2019/08/26/747248636/persistent-engagement-the-phrase-driving-a-more-assertive-u-s-spy-agency?t=1583919442321

National Cyber Security Centre. (23 October 2019). *Annual Review 2019*

National Security Agency. (n.d.). *Understanding the Threat*, https://www.nsa.gov/what-we-do/understanding-the-threat/

New Zealand Government. (June 2011). *National Cyber Security Strategy*

New Zealand Government. (10 December 2015). *New Zealand's Cyber Security*

New Zealand Security Intelligence Service. (2017). *History*, https://www.nzsis.govt.nz/about-us/nzsis-history/

O'Brien, C. (2007). Politics of Intelligence: How the Politicisation of the Intelligence Cycle Undermines the Integrity of Australia's Intelligence Agencies, *Journal of the Australian Institute of Professional Intelligence Officers*, *15*(3), pp. 58-68

Office of the Director of National Intelligence. (January 6 2017). *Assessing Russian Activities and Intentions in Recent US Elections*. National Intelligence Council

Pepper, D. (2010). The Business of Sigint: The Role of Modern Management in the Transformation of GCHQ, *Public Policy and Administration*, *25(*1), pp. 85-97

Peritz, A. J. & Rosenbach, E. (2009). *Confrontation or Collaboration? Congress and the Intelligence Community*, Belfer Center for Science and International Affairs

Petit, P. (2019). 'Everywhere Surveillance': Global Surveillance Regimes as Techno-Securitization, *Science as Culture*, *29(*1), pp. 30-56

Porter, P. (2016). Taking Uncertainty Seriously: Classical Realism and National Security, *European Journal of International Security*, *1(*2), pp. 239-260

Savage, C. (2018). *N.S.A. Triples Collection of Data from U.S. Phone Companies*, https://www.nytimes.com/2018/05/04/us/politics/nsa-surveillance-2017-annual-report.html

Schmitt, M. N. (2017). Respect for Sovereignty in Cyberspace, *Texas Law Review*, *95*(7), pp. 1639-1670

Sciutto, J. (28 June 2017*). How One Typo Helped Let Russian Hackers In*. CNN, https://edition.cnn.com/2017/06/27/politics/russia-dnc-hacking-csr/index.html

Slayton, R. (2017). What is the Cyber Offense-Defense Balance?: Conceptions, Causes, and Assessment, *International* Security, *41(*3), pp. 72-109

Soesanto, S. (2018). *No Middle Ground: Moving On From The Crypto Wars*, European Council on Foreign Relations

The NATO Cooperative Cyber Defence Centre of Excellence. (2020). *Tallinn Manual 2.0*, https://ccdcoe.org/research/tallinn-manual/

The Wall Street Journal (29 July 2004). *Cisco, Huawei Settle Lawsuit*, http://www.wsj.com/articles/SB10910232814167631

United Kingdom Government. (1 November 2016). *National Cyber Security Strategy 2016-2021*

Watt, E. (2017). The Right to Privacy and the Future of Mass Surveillance, *The International Journal of Human Rights*, *21(*7), pp. 773-399

Whibley, J. (2014) One Community, Many Agencies: Administrative Development in New Zealand's Intelligence Services, *Intelligence and National Security*, *29*(1), pp. 122-135

Williams, C. (30 March 2009). *Spy Chiefs Warn Over Huawei Gear in 21CN*, theregister.co.uk, http://www.theregister.co.uk/2009/03/30/huawei_threat/