MSc SECINTEL Independent Study (Dissertation)

CHARLES UNIVERSITY

National Resilience in Cyberspace:

The United Kingdom's National Cyber Security Strategy Evolving Response to Dynamic Cyber Security Challenges

31st July 2018

2263260J

22447459

Presented in partial fulfilment of the requirement for the Degree of MSc International Security, Intelligence and Strategic Studies (SECINTEL)

Word Count: 22,094

Supervisor UofG: Dr. Eamonn Butler

Supervisor Charles Uni: Dr. Vitek Stritecky

MSc SECINTEL Independent Study (Dissertation)

CHARLES UNIVERSITY

MSc International Security, Intelligence and Strategic Studies

2017-2019

Dissertation Archive Permission Form

I give the School of Social and Political Sciences, University of Glasgow permission to archive an e-copy/soft-bound copy of my MSc dissertation in a publicly available folder and to use it for educational purposes in the future.

Student Name (BLOCK LETTERS): __KAILYN JOHNSON_____

Student Number: ___2263260J_____

Student Signature: _____ Date: __25th July 2018__

PLEASE INCLUDE A COPY OF THIS FORM WITH THE SUBMITTED SOFT-BOUND COPY OF YOUR DISSERTATION.

Abstract: Criminals and other threat actors are adapting to the growing reliance individuals, organisations, and nations have upon technology and the internet and have augmented their capabilities to be oriented in that direction for malevolent purposes. Cyberspace has become an extremely large vulnerability for countries because it facilitates any person with access to a computer or other technology along with malicious intent, to cause harm. The increased risk people and organisations now face in cyberspace is not isolated to just them. Nations now are also at an increased risk because of the evolving ubiquity of cyberspace and technology. States are at risk of cyber threats because of vulnerabilities in individual citizens and organisations. Nations have now become intended targets by a larger spectrum of threat actors. This research examines how the United Kingdom has developed their specific national cyber security strategy to improve national resilience to threats, and how well the UK government adapts to an ever-changing threat landscape. The UK is still deficient in the appropriate and thorough execution of their proposed strategies and strategic policies to attain national resilience and security. There have been strides to achieve that goal, but the national strategy continues to fail to contextualise past cyber-attacks and input those lessons into practice. Until the UK can develop and implement strategy that is up-to-date with the current trends in cyber threats at a quicker pace, they will not be able to maintain resilience or security in cyberspace.

Table of Contents

Chapter 1: Introduction

Cyberspace has become one of the most frequently utilised platforms where security threats are conducted. The internet has allowed for instant and expansive connectivity between individuals across the world. Most of daily life now occurs in cyberspace: business transactions, communication between friends and family, banking, education, and learning, amongst many others. With that, though, means that criminals and other threat actors are also adapting to the increasing reliance upon cyberspace to enhance their abilities to cause havoc. Cyberspace has become an extremely large vulnerability to individuals, organisations, and nations that facilitates any person with access to a computer or other technology along with malicious intent, to cause harm. Threat actors are developing new methods for threat activity quickly, and are learning how to exploit even minor vulnerabilities in either technical systems or human tendencies that allow the perpetrators to cause their intended damage. The rise of cryptocurrency and the fact it is difficult, if not impossible to trace because of the decentralisation of it (Corcoran, 2018), means threat actors have quickly adapted and learned how to exploit this new form of currency and make illicit profits. Threats to various levels of security have grown exponentially due to cyberspace, which has resulted in the increased use and development of cyber security policies to mitigate these new and often-times unknown threats and vulnerabilities.

Many organisations have begun to develop and implement cyber-oriented policies into their security practices to combat the rise of cyber threats. The past few years have seen an increasing shift in organisations towards having various types of policies that have been put into place to counteract cyber threats. This is especially true following the rise of significant large-scaled data breaches that have occurred such as the Sony data leak in 2014, the Yahoo data breach in 2013, or the more recent Equifax leak (Armerding, 2018). These leaks have demonstrated to both businesses and individuals that people must actively engage in proper security-literate behaviours to lessen the risk of these incidents affecting them. Following these events, and others like them, more organisations have begun to see the utility in antivirus software, better informed and trained employees, and other security practices that can reduce their risk in cyberspace. With the increase necessity for improved cyber security practices, there has also been an increased need for more research to be conducted to examine where vulnerabilities lie and how to attempt to fix them. Academia has become extremely active in

conducting a variety of research that aims to understand cyber security risks in both technology and people, as well as develop comprehensive solutions to these threats.

The increased risk people and organisations now face in cyberspace is not isolated to just them. Nations now are also at an increased risk because of the evolving ubiquity of cyberspace and technology. States are at risk of cyber threats because of vulnerabilities in individual citizens and organisations. Nations have now become intended targets by a larger spectrum of threat actors. In particular, traditional espionage has become somewhat a thing of the past with the stereotypical 'spies', conducted in a 'textbook' manner. The antiquated platform of espionage has evolved with the development of technology and is now more frequently observed being conducted in cyberspace. Threat actors, both state-sponsored and not, can now damage the security of a nation without leaving the safety of their own home. Technology has become a more prevalent platform as daily life is becoming more enmeshed with the digital world. Controlling infrastructure, data storage, and other aspects of communication sharing, national security strategies are now needing to adapt and take into consideration these threats that are often unseen and difficult to predict. Policymakers have had to create and implement strategy that is specific to cyber security, especially to ensure the future security of a nation.

Objectives of this research

With the rise of cyber risks threatening the security of nations and their people, more governments are intent on developing a comprehensive strategy that accounts for cyber threats and directly addresses methods to mitigate the risks. This research will be examining how the United Kingdom (UK) has developed their specific national cyber security strategy to improve national resilience to threats, and how well the UK government adapts to an ever-changing threat landscape. The research will analyse how the government has developed their cyber security strategy to accurately mirror the threats it faces and if it will address if the strategy is implemented at a pace that keeps the nation from falling behind threat actors and if the strategies are proactive. The research will utilise three significant cyber events that have occurred in the past decade to attempt to understand if the lessons learned from those incidents were then taken and translated into strategy in the form of specific policies, new organisations, documents, etc. This should provide insight as to how the UK is fairing in maintaining national resilience in an uncertain threat environment, and if the government is reacting swiftly enough to handle new and constantly changing cyber threats. To accomplish this, the research will use the three cyber

incidents and line them up with the publications of the national cyber security strategy and other Parliamentary documents to examine the steps that are being taken to preserve national security.

Chapter 2: Literature Review

Since there is little research currently analysing the UK's national cyber security strategy and its ability to ensure security and resilience, I aim to use a strategic culture theoretical framework to answer the research question: how has UK national cyber security strategy evolved to address and ensure national resilience in the face of dynamic cyber security challenges? I also intend to fill the gap in research that examines if and how specific cyber incidents have influenced the evolution of national cyber security strategy, as well as if those strategies have become more proactive in execution rather than reactionary. This research intends to understand the process by which the first published UK national cyber security strategy changed to account for the changing threats to the UK and their vulnerabilities as technology and tactics grow increasingly sophisticated. This section will examine past literature on a variety of topics that will help inform my research and analysis on the UK's cyber security strategy evolution with current cyber security trends.

2.1 Strategic culture

Strategic culture is the theoretical framework that this entire paper will be founded upon, so it is crucial to delve into what strategic culture is, as it has many definitions and uses in a geopolitical context. It will then also be necessary to discuss cyber strategic culture, even though it is not necessarily an officially coined term, since this research will utilise strategic culture from a cyber perspective as the foundation for analysis.

Strategic culture has a variety of definitions depending on who is asked, despite the commonalities they all share regarding the over-arching theme of integrating culture with national policies (Margaras, 2004). Initially, strategic culture was used to examine nuclear deterrence strategy in relation to the Soviet Union in the 1970s and ascertain if it was able to effectively anticipate Soviet movement (Margaras, 2004: 1). Analysts were not able to sufficiently make these predictions because of failure to utilise a theoretical framework that mirrored reality (Margaras, 2004: 1). Researchers later determined that due to cultural differences and varying national interests, nations will engage differently, so there needed to be a new tool that grasped that but could still be applicable across the board (Margaras, 2004: 1-2). The strategic culture research narrative has seen multiple adaptations of ideals that were influenced by the era that they were coined in and utilised (Margaras, 2004: 1-2).

The first so-called ‘generation’ of strategic culture was heavily influenced by the Cold War (Margaras, 2004). During this time period, Synder interpreted strategic culture as ‘the sum of ideas, conditioned emotional responses, and patterns of habitual behaviour that members of a national strategic community share with regard to nuclear strategy’ (Snyder, 1977: 8 as cited in Longhurst, 2000: 302). Synder attempted to coalesce feelings and behaviours with strategy development to show that strategy does not exist in a vacuum and needs to consider both the human aspects of the policymakers as well as the ‘enemy’ it is built to be strategic against (Margaras, 2004: 2-5). Another prominent definition used for strategic culture was devised by Colin Gray who stated that strategic culture was ‘the modes of thoughts and action respective to force, derived from the perception of national historical experience’ (Gray, 1986, as cited in Margaras, 2004: 2-4). This definition was crucial to future development because it suggested that strategic culture could help explain certain state behaviours which might not be considered as ‘rational’ (Margaras, 2004: 2-3). This idea intended to help explain why states were not always rational actors as an extension of Morgenthau’s concept for international relations. Realism, as it is known, posited that politics and engagement between nations in the international community stemmed from human influences (Morgenthau, 1978: 4-15), so this definition of strategic culture helped take this further by attempting to explain what sort of human-based concepts influence strategic decisions.

Alastair Iain Johnston stated that ‘strategic culture is an ideational milieu of shared assumptions and decision rules that impose a degree of order on individual and group conceptions of their relationship to their social, political, or organisational environment which can limit behaviour choices’ (Johnston, 1995: 33-64). Here, Johnston suggests that strategic culture has to have assumptions regarding the enemy and they threat they pose integrated with assumptions on one’s own ability to use force to diminish the enemy threat (Johnston, 1995: 33-64; Margaras, 2004) which he oriented this definition to be applicable toward Russian adversaries. There are at least another four different definitions given to strategic culture (Margaras, 2004) to help conceptualise the term and give it utility. Understanding that the common theme amongst all of the variants is that strategy is influenced by the culture and specific historical context of the particular nation it originates from. This understanding of the variants of definitions and the context it has stemmed from then assists the reader in understanding what cyber strategic culture is and how it is utilised.

The concept of cyber strategic culture is not a common term specifically found in much previous research. Kenneth Geers is one researcher who attempts to apply concepts from strategic culture to the contemporary field of cyber security. He notes that cyber-attacks are not necessarily the ultimate threat in itself, but rather the use of cyber-attacks as a means to achieve a greater objective, is an innovative, key national security problem (Geers, 2011: 9). The internet has not only allowed for a new mechanism for attacks and threats to be delivered to nations, but it also could become the newest battlefield states will have to play upon to ensure their own security (Geers, 2011: 9-10). Due to the increasing connectivity of the world via the internet and the ease of access to it, nations now have to develop comprehensive security strategies that do not just consider nation-states, but also smaller-scaled actors, such as terrorist organisations, hacktivist groups, and even malicious individuals (Geers, 2011: 9-16). National strategy for cyber security has to be comprehensive where nations create both cyber defensive capabilities and cyber offensive capabilities (Geers, 2011). Threats no longer can be simply apprehended through border control, diplomatic relations, and strategic partnerships; threats can permeate borders easily now with the internet and advancements with technology, and, as Geers points out, governments must make proportionate investments in cyber incident response, technical training for employees in all sectors, enhanced network security, and international cooperation to adequate attempt to mitigate those new threats (Geers, 2011). Geers and his statements regarding cyber security and strategy are beneficial to help guide this research's analysis into national cyber security strategies development and adaptations based on constantly evolving cyber threats and incidents. Understanding how cyber security can be strategic and what sort of strategies Geers postulates are important to improve national security (Geers, 2011), will facilitate the analysis of the UK's strategies by examining the government's ability to amalgamate a variety of resources and fields to improve the nation's resilience and protection.

2.2 Human-Centred Security

It is mutually agreed upon by many that humans are the greatest cyber security vulnerability organisations and companies have. As Mark Hall stated, 'people are inconsistent' (Hall, 2016: 9) and because of this, it is a major area of concern for organisations' security (Hall, 2016: 9) as well as national security. Most companies have security policies that are inconsistent and not in accordance with how people work (Waldrop, 2016). People are not like machines and must attempt to balance the demands of completing their primary tasks with secondary tasks, like

cyber security tasks, which creates a dilemma for employees of which is more important (Beautement et al., 2016). Employees can struggle to multitask between their productivity on their individual work and security responsibilities that might not necessarily be deemed as immediately necessary (Beautement et al., 2016). The concept of human-centred security is crucial to comprehend because people are central to both the creation and development of national security, as well as the implementation of it. Understanding how people work in accordance to cyber security procedures is necessary to create successful strategy. Strategy is useless unless people actually engage in the policies and processes identified in it. This section will look at an assortment of research that has already been conducted examining different aspects of human-related concepts and human influences on cyber security which will benefit this research's analysis related to the UK's ability to develop dynamic and relevant security measures to ensure national cyber security.

2.3 Security Awareness Training

As the amount of cyber-attacks targeting both nations and the private sector continue to rise, more research has been conducted how cyber security awareness training can help improve security. Bowen, Devarajan and Stolfo's article mentions that through awareness training, computer users can learn how to distinguish and combat cyber threats, particularly malware and phishing attempts (Bowen, et al., 2011: 230-231). On a similar note, Abawajy stated that people are organisations' most robust defence mechanism against security threats, but only if the employees are properly trained (Abawajy, 2014: 236). He observed that the main cause of data breaches in organisations occur because of employee negligence. Appropriate security awareness training for employees can combat these unsafe cyber practises that exacerbate businesses vulnerabilities (Abawajy, 2014: 236-238). Video-based educational security exercises were found to be the most effective method for awareness training because researchers found that employees' ability to detect email-based phishing attempts increased with this type of training, but the research also found that interactive, game-based training also produced improved cyber habits for employees (Abawajy, 2014: 245-247). All in all, cyber security awareness training enabled employees to generate smarter choices through increasing their cyber security knowledge which helps safeguard companies from unnecessary security threats (Abawajy, 2014: 246-247). The conclusions from these past studies are good background to have when then analysing the UK's national cyber security strategies because national strategy also often

includes plans on how to better secure the private to maintain comprehensive national protection. National cyber security strategy has to recognise the already-present struggles and successes cyber security training has for organisations and utilise that to then inform recommendations for the strategy that aims to be implemented. This research anticipates that the UK's national cyber security strategies will include some form of private sector security training, so this is important to understand.

Although the average populace recognises that cyber threats exist, and they must be aware of them, it does not prevent them from engaging in unsafe cyber behaviours. The 'privacy paradox', as discussed in an article by Kearney and Kruger, is the discrepancy between individuals have a high level of security awareness who heavily value their privacy, can still be easily coerced to disclose personal or other confidential information to unknown people (Kearney and Kruger, 2016: 47). They conducted an experiment to examine an organisation's employees' ability to identify phishing scams which lead to surprising results: a large portion of employees revealed their personal details when prompted by phishing schemes (Kearney and Kruger, 2016: 48-56). Their experiment also uncovered that newer employees who have been in a company for a shorter time, tended to be targeted more frequently than others, although researchers still saw a substantial number of employees with higher levels of work experience fall victim to phishing schemes (Kearney and Kruger, 2016: 48-56) meaning that no one is wholly exempt or safe from cyber threats. This study accentuated the significance recurrent security awareness training can have for both employees and management due to the fact there is too much reliance put on the physical security of systems to protect organisation and governmental departments as a whole (Kearney and Kruger, 2016: 48-56). People still fell victim to phishing attacks even with the proper security training so more needs to be researched and done on this topic (Kearney and Kruger, 2016: 48-56). It is obvious that more research should be conducted on how to address this so-called 'privacy paradox' that organisations are victim to despite having security awareness trainings given to employees, though this will not be examined specifically in this paper. These findings regarding the 'privacy paradox' will help this research comprehend that lower-level employee behaviours, alongside other people and their habits within an organisation, can all be targeted for cyber-attacks. Anyone can be a target, which means that the case studies analysed are crucial to recognising that breaches at any level in an organisation or government office can be a result of poor diligence and other inadequate cyber

security behaviours. This will help inform cyber security strategy at a national level that this issue must remain a key problem to continually address in policy and strategy as a whole to ensure security.

2.4 Understanding the Attacker

There has been research conducted focused upon the attacker and their own behaviour to attempt to understand how they work, think, and why they engage in cyber-crime. This information has then been used to help generate new methods to mitigate hacking and cyber threats. Using attacks trees and nodes to produce attack paths, Orojloo and Azgomi tried to predict how attackers would possible behave (Orojloo and Azgomi, 2016: 6111-6136). They discovered that to direct an attack, an attacker must have access to a system to a certain extent as well as a sufficient amount of knowledge on the specific system's mechanics (Orojloo and Azgomi, 2016: 6111-6136). It is also necessary for attackers to recognise the circumstances when it is necessary to use password or brute force techniques versus implementing malware, as well as they need the required skill set for the particular system they are trying to gain access to (Orojloo and Azgomi, 2016: 6111-6136). Using the criminological perspective, Wada, Longe, and Danquah examined the social behaviour of cyber criminals. Through the application of criminological theories in the analysis of cyber criminals' behaviour, they discovered that cyber-crime allows for dissociation from the victims, eliminating any guilt or compassion that can be associated with crimes which involve some form of physical contact with the victim (Wada et al., 1970: 1-12). Cyber-crime allows for the attacker to remain anonymous and untraceable (Wada et al., 1970: 1-12), and there lacks a strong degree of physical deterrence from cyber-crime due to the connectivity through the Internet, which creates more opportunity for criminals to participate in it (Wada et al., 1970: 1-12).

2.4.1 Political-based hacker

In a study done by Holt et al., they interviewed ten Turkish hackers to better understand their rationale behind doing what they do (Holt et al., 2017). The hackers all had some sort of ideological reasoning behind their hacking targets. Many of the hackers interviewed stated that they were Turkish nationalists with strong Islamic values which influenced who they then targeted to hack (Holt et al., 2017: 224). One interviewer stated that they chose targets that were 'enemies of Muslims', terrorism-sponsored sites, or politically opposite to their own ideals like the Turkish separatist group, the PKK (Holt et al., 2017: 224). Ideology is extremely influential

for many attackers in whom they target and why, as seen with this case study as well as in real-life with groups like Anonymous. While ideology is a significant factor for hackers, it is not the only thing that influences why people choose to become hackers. Politically-motivated attackers and their hacking patterns that Holt et al. uncovered in their research might be beneficial in the case study analysis of the NotPetya cyber-attack because many believe it was a politically-motivated attack as 70-80 percent of those affected were in the Ukraine, specifically government offices and certain critical infrastructure (Protectimus Solutions, 2017). This foundation of what politically-motivated hackers look for when choosing targets and how they put forth an attack will be extremely useful in this research because national cyber security strategies need to understand who they are trying to secure the nation-state from.

In the same article by Holt et al., they found that interest in technology from an early age had an impact on their future development into hacking (Holt et al., 2017: 219-220). The more exposure these people had to computers and the Internet, the more their interest grew which then caused them to reach out to learn more about the systems themselves hacking (Holt et al., 2017: 220). Knowledge sharing was notably key for potential hackers to get the exposure to technology and develop their skills further (Holt et al., 2017: 220). Many of the hackers interviewed stated that there are a variety of forums and tutorials by other hackers found on the Internet that help teach certain skills or advance current skills (Holt et al., 2017: 220). This increases the Turkish hackers' skill, which they can then add their own twist eventually to attack techniques to make it their own (Holt et al., 2017: 220). This network of hackers helping hackers allows knowledge to be spread, which can lead to a greater threat for organisations. On top of that, attackers that are ideologically motivated with the appropriate hacking skills, can cause significant damage to companies. It is important to have an understanding regarding the potential reasons for why attackers target specific organisations as well as how they learn the skills to do so because that can help inform potential targets about what they need to be aware of. This research will not necessarily expand much upon the attackers of each cyber-attack nor the specific, simply because the three attacks analysed in this study do not have officially agreed upon and/or identified attackers. However, understanding some of the key processes for threat actors in general can still be beneficial for informing and developing comprehensive security strategies at a national level, especially regarding threat actors with political motivations. This is also beneficial background to acknowledge because future research could be conducted by the National Cyber Security

Centre, the National Crime Agency, and UK-based academia to further examine motivations for various threat actors which could significantly help the UK government develop thorough and well-rounded national cyber security strategies and policies to combat them more effectively.

2.5 The Copenhagen School

The Copenhagen school of thought in international relations focuses upon expanding the security agenda to not only focus upon military security, but to also bring in political, economic, societal, and ecological factors in a post-Cold War era (Booth, 2007: 32). A major part of the security agenda focuses upon the securitisation of words and actions, and how that plays into the greater security context (Booth, 2007: 33). Hansen and Nissenbaum utilise the Copenhagen school of thought to discuss how cyber security has come about and its importance. They begin by discussing how the cyber realm has become securitised, both the word itself and the actual domain (Hansen and Nissenbaum, 2009). The term 'cyber security' immediately securitises cyber space by creating the belief that there is a complex public, private, and governmental responsibility to making cyber space safe (Hansen and Nissenbaum, 2009: 8). Many people are currently complacent to creating and maintaining cyber security, despite their exposure to many cyber threats (Hansen and Nissenbaum, 2009: 8). This discourse is meant to securitise the cyber world for average people and authorities alike because of the increase in exposure to cyber threats that have not seen an equivalent increase in countermeasures to combat those threats (Hansen and Nissenbaum, 2009: 8). Because the internet allows the world to be more connected, this heightens the potential risk since the damage can have a world-wide impact through the connected networks (Hansen and Nissenbaum, 2009: 10). Hansen and Nissenbaum discuss how the 2007 cyber-attack in Estonia laid the foundation for the hyper-securitisation of cyber security (Hansen and Nissenbaum, 2009). The country experienced a large-scaled Distributed Denial of Service (DDoS) attack that broke down a variety of networks where the government could not interact with each other, citizens could not get in touch with authorities, media outlets could not update what was happening, and crucial transactions like banking were completely halted (Hansen and Nissenbaum, 2009). This set a precedent for what would potentially be affected if a cyber-attack occurred, because nothing like it happened before. This attack indicated that everyday life can be as monumentally affected as governments are in cyber-attacks, which laid the foundation for hyper-securitisation of cyber space to occur (Hansen and Nissenbaum, 2009). It created the understanding that cyber threats are real and can have massive implications for

society as a whole if vulnerabilities are not addressed in cyber space (Hansen and Nissenbaum, 2009). Following the Estonia attack and with recent, new cyber-attacks, people can see the damage caused via technology and cyber space which has led to the uptake of CSIRTs (discussed in more detail later), information security teams, and more comprehensive cyber security policies within organisations. The securitisation of cyber space and the actors within it has allowed for the discourse of cyber security to come about; however, with the expansion of internet-based technology and people's and government's growing reliance upon those, this has created more vulnerabilities that could be exploited by threat actors. The securitisation of the cyber world is necessary, but most people, policymakers in particular, still do not act in a security-conscious manner when engaging with vulnerabilities and internet-facing technology. This has allowed cyber threats to remain a major risk to individuals, organisations, and governments that are not fully understood or fully protected against. The hyper-securitisation of the cyber realm has not necessarily created the proper number of countermeasures against it. Specifically, countermeasures at a national level that develop at a sufficient pace to mitigate current and future threats as well as the creation of pre-emptive strategies to get ahead of threat actors are necessary.

Using the Copenhagen school of thought for security, securitising the word 'cyber' and the space it exists in has led to a massive new industry to safeguard organisations, nation-states, and individuals from crime; however, this has also created an expectation and reliance upon governments, organisations, and security protocols likes anti-virus software, etc. to be the sole source of protection. Individuals are not cognizant of their own cyber behaviours that diminish cyber safety and assume that just having software and 'secure' systems are enough. This dissonance will be exemplified in this case study and policy development analysis. I anticipate the research will show that people do not necessarily properly use cyber threat countermeasures despite the increased vulnerability all people are exposed to due to the sophistication of technology and attacks, and the pervasiveness the internet and technology have in daily life. This often results in government bodies and officials not necessarily creating national strategy that will be put into practice by all parties necessary to improve security and resilience. Officials not recognising individual failings in preventative and appropriate cyber security habits are a major source of national insecurity.

2.6 CSIRTs and Attack Detection

Since the late 1980s, a majority of organisation have integrated teams that are specifically built to address cyber security issues that arise within the organisation. These teams are called Computer Security Incident Response Teams or CSIRTs (Alberts et al., 2004: 1). CSIRTs are utilised for formal incident responses and have a variety of roles they take on such as cyber security policy making, analysis for possible incidents, and head the coordination for when a real security incident takes place (Alberts et al., 2004: 1-2). CSIRTs have now become engrained in and built into a majority of organisations. CSIRTs are located at every level, with there being internal company CSIRTs, governmental CSIRTs, and national CSIRTs (Alberts et al., 2004: 1-3). Depending on the type of security incident, these CSIRTs will engage with each other to mitigate the incident, prevent it from spreading, as well as address the consequences of it (Duračinská, 2017). CSIRTs are crucial for the detection of cyber threats, the mitigation of them, as well as creating policy to improve cyber security. CSIRTs at a national level are a necessity to act as a liaison between organisational CSIRTs, international CSIRT bodies, and the nation it is built to protect to better inform strategy and policy that is essential for national resilience.

Asher and Gonzalez examine whether CSIRTs and trained Security Operation Centres (SOCs) are better at detecting attacks compared to the average employee to see how to better improve attack detection and training (Asher and Gonzalez, 2015). Their experiment uses an intrusion detection system tool that is supposed to detect network intrusions and network misuse automatically which then sends those red flags to analysts to investigate further (Asher and Gonzalez, 2015). They looked to see if trained experts were better at detecting legitimate attacks compared to regular employees. They found that experts and novices were fairly similar in their positive detection rate and confidence in those responses (Asher and Gonzalez, 2015). The findings of this suggest that experts are no matter than employees at discovering legitimate threats and malicious attacks (Asher and Gonzalez, 2015). Despite this, there is still a necessity for security experts, as technology evolves quickly and with that, cyber threats evolve and become more sophisticated. CSIRTs and SOCs continually train and stay up-to-date with the newest threats and vulnerabilities companies might face. This makes them a useful tool for organisations, so those vulnerabilities are managed to enable regular employees to focus on their day-to-day work. Asher and Gonzalez state that CSIRTs and security analysts must make pragmatic decisions and understand a plethora of complex, independent attributes related to

cyber security which requires them to have academic knowledge and situational knowledge gained through experience to successfully detect and mitigate cyber threats or attacks (Asher and Gonzalez, 2015). This exemplifies the necessity for trained security experts in organisations and governments to maintain strong and stable cyber security. However, as recent cyber incidents have exposed, which will be further analysed in this research, simply having secure systems and trained experts does not mean that a state is completely exempt from experiencing attacks. There is also a necessity for having security-aware citizens, individual government officials, commercial organisations, and other organisational bodies as they all have crucial vulnerabilities to address. This research will aim to see if the interaction between security teams, people, and government bodies through awareness trainings, proactive policies, etc. does in fact improve national security, or, if due to poor cyber habits at every level regardless of training, and a lack of adequately understanding strategies to mitigate threats, nations are still left vulnerable as seen in the cases that will be examined in-depth in this research.

2.7 Ransomware

Considerable research has been conducted on various forms of cyber extortion attacks, specifically distributed denial-of-service (DDoS) attacks and ransomware (malware) attacks. DDoS attacks overwork systems by overwhelming it with several simultaneous requests from computers of random people that have been hijacked resulting in a system failure (www.digitalattackmap; Sulkowski, 2007: 22). Sulkowski mentions in his article that once attackers penetrate networks through DDoS attacks, businesses then become liable to their customers since the attackers can gain access to private customer data (Sulkowski, 2007: 22). This then has the potential to cause millions of dollars in deficits for businesses through legal ramifications (Sulkowski, 2007: 23). DDoS attacks caused more than $26 million in losses for businesses in 2004 alone because of the legal ramifications and revenue lost from the shutdown of their systems (Sulkowski, 2007: 23). Comparably, Norton Symantec, the cyber security software company, documented that between 2013 and 2016 Business Email Compromise phishing scams, a specific type of ransomware cyber-attack, cost businesses over three billion dollars in damages and deficits (Symantec, 2017: 24-28). Cyber extortion threats and attacks will continue to increase in frequency as well as affect a wider span of people and become more damaging to businesses and governments. This means additional research is necessary in order to combat these rising problems. A DDoS attack is just one method cyber-attacks can present.

Other methods will be discussed in the next section to give the reader a solid foundation on the variety of ways a cyber-attack can occur. This will be useful in understanding the case studies and the development of national cyber security strategies that will be investigated in this research.

2.8 Social Engineering

Spear phishing or, simply, phishing is one of the more common, if not the most common, methods threat actors use to initiate an attack. To successfully use phishing as an initial attack vector, threat actors have to constantly construct complex and realistic ruses that will force targets to believe their legitimacy and either click on the link provided in the scam or give the threat actor the credentials they are wanting (Webroot.com, 2018). This form of manipulation is called social engineering and it can materialise in a variety of ways depending on the intent of a threat actor and their capabilities. Phishing can be in the form of an email with a malicious application or downloadable document and threat actors have learned to produce emails and requests to potential victims that contain specific semantics that make them appear legitimate to the victim and bypass spam filter algorithms (Bowen et al., 2011). This tricks the victim into opening the link, downloading the document, or revealing confidential credentials, granting a threat actor access into the network (Bowen et al., 2011). Improved language in phishing ruses has elevated the probability of success for actors, which accentuates the necessity for strategy to recognise this serious vulnerability.

Threat actors also exploit psychological and technological vulnerabilities of potential victims to employ their malware implementation through phishing and other social engineering tactics (Ovelgönne et al, 2017: 51:1-2). Human error and weakness account for a substantial portion of risks to security at a national, organisational, and individual level (Ovelgönne et al, 2017: 51:2-3). Similar to the conclusions in an earlier section regarding the 'privacy paradox,' it is interesting to note that even people who are highly computer literate and well-trained remain a security threat to the organisation, government, etc. just as lower-level personnel and those with little to zero technical background are (Ovelgönne et al, 2017: 51:5-6). This could be a result of optimism bias, which is the discrepancy between a person's expectation of an anticipated outcome and the actual outcome (Sharot, 2011: R941-R945). This phenomenon can sometimes be seen in people who have high levels of computer security knowledge and training and engage in deviant cyber behaviours (Pfleeger and Caputo, 2012). This could be due to the assumption

that ‘it will not happen to me’ because they have cyber security knowledge and may be over-confident in their own ability to avoid and mitigate succumbing to threat actors’ ploys. This will be important to remember when analysing the UK’s development of their cyber security strategies because the government needs to remain cognizant that anyone is vulnerable and a potential target to social engineering schemes. These can have severe negative repercussions for national security.

While phishing is the most utilised attack vector currently, it is not the only form of social engineering and method of infiltrating systems, especially national-level networks and enterprises. Another prevalent social engineering tactic threat actors can use, specifically state-sponsored threat actors or threat actors with political interests, is a watering hole attack. This is where a threat actor compromises a specific website(s) by inserting an exploit into the website which will then take advantage of a visitor’s software vulnerability to install malware, usually in the form of a Remote Access Trojan (RAT) (Abendan II, 2013). This RAT then allows a threat actor to access any data and take control of the infected system (Abendan II, 2013). Typically, watering hole attacks are used in targeted attacks, as the threat actor has to determine which websites to compromise based on what they are intending to gain from the attack (Abendan II, 2013). These are often seen used for cyber espionage because of the precise targeting nature of the attack vector (Abendan II, 2013).

Chapter 3: Methodology

3.1 Strategic Culture

Strategic culture and the concepts and idea that fall under it will guide this research and its theoretical framework. This perspective will help drive the data collection and analysis process. It will be used to examine how the UK government conceptualises cyber security phenomena and then implements government strategy to combat those perceived threats. While there is not a fully agreed-upon definition for strategic culture, this research will utilise the definition from Nayef Al-Rodhan which is: 'an attempt to integrate cultural considerations, cumulative historical memory, and their influences in the analysis of states' security policies and international relations (Al-Rodhan, 2015: 1). This definition will then be operationalised as cyber strategic culture where the above definition goes a step further by specifically directing the amalgamation of culture, history, and national interests to cyberspace. Strategic culture, in general, offers a theoretical lens to better understand the similarities behind international problems and a state's motivations for specific actions (Al-Rodhan, 2015: 1). This theoretical paradigm will be used to orient this research due to the recognition that strategy development is largely influenced by both the culture of the party building strategy as well as national interests (Al-Rodhan, 2015). The interaction of the two motivate and manipulate the direction of development and implementation (Al-Rodhan, 2015). In relation to cyber security specifically, this model will assist in creating a new historical memory from national experience (Gray, 1986 cited in Margaras, 2004: 2) to cyber incidents as they are fairly new threats to security. These require an innovative integration of ideals, new responses, and habitual behaviours (Synder, 1997 cited in Al-Rodhan, 2015: 1-3) to address this new strategic landscape. In particular, the research will utilise cyber strategic culture as the underlying narrative to drive analysis because, as Kenneth Geers states, 'cyber-attacks on critical infrastructure and institutions are strategic by nature, so the response must be equally strategic to effectively counter those threats' (Geers, 2011: 29). This research will aim to answer the question: how has UK national cyber security strategy evolved to address and ensure national resilience in the face of dynamic cyber security challenges?

3.2 Comparative Case Study Analysis

To answer this question, I will conduct a comparative case study analysis of three past cyber-attacks in conjunction with a policy development analysis. A comparative analysis of these

various case studies in conjunction with an analysis into strategy development and implementation, will be a beneficial in gaining a rich insight into the progression of the UK's national security strategies based on the evolving threat environment. This insight will help to examine how the UK is fairing in ensuring national security and resilience in cyberspace through the development of those strategies.

A comparative case study analysis is an expansion upon case study research which has been defined and utilised as a useful research method in the past thirty years. It takes qualitative case study research further by amalgamating micro, macro, and meso dimensions of case-based research (Bartlett and Vavrus, 2017: 6). This method allows for a more comprehensive analysis and understanding of the cases it is examining. This method is notably different from the usual case study analysis in the fact that it is a more pragmatic approach to understanding culture, context, time, and place with a multidisciplinary perspective (Bartlett and Vavrus, 2017: 6). It utilises two different concepts of comparison. It identifies specific units of analysis and compares and contrasts it, as well as using processual logic to draw across groups, places, people, and time (Bartlett and Vavrus, 2017: 8). This is new because the method not only compares and contrasts between various case studies and the variable(s) it is examining, but it also addresses how specific factors are important to the process/scenarios (Bartlett and Vavrus, 2017: 8). Comparative case study analysis aims to go beyond dichotomies, unchanging classifications, and archaic concepts of what is going on in the world (Bartlett and Vavrus, 2017: 10). In doing this, the analysis examines social actors, language, discourse, institutions, and policy on top of the usual case study variables to understand how these factors influence the circumstances by which things occur (Bartlett and Vavrus, 2017: 10). To do this, comparative case study analysis utilises critical theory which critiques inequality and change in society by studying the practices and processes of power, exploitation, and agency (Bartlett and Vavrus, 2017: 11). This emphasises the importance of social interactions and context (Bartlett and Vavrus, 2017: 12). To examine context, researchers state that activity is context (Bartlett and Vavrus, 2017: 12). Various social relations and networks constitute context, which is then studied to understand how social interactions, economic developments, and political processes have been shaped by those social relations and networks (Bartlett and Vavrus, 2017: 12-13). Crucial to the comparative case study analysis is that comparisons between the cases are made three different ways: vertical, horizontal, and transversal (Bartlett and Vavrus, 2017: 14). Vertical comparisons examine

influences at different levels such as international, local, and regional amongst others, that impact a case (Bartlett and Vavrus, 2017: 14). Horizontal comparisons look at the contrasts between the various cases and sees what links can be made between the cases regarding the social actors, documents, and other influences (Bartlett and Vavrus, 2017: 14). Lastly, transverse comparison attempts to compare the cases over time, which can be much more difficult if the cases are not longitudinally studied (Bartlett and Vavrus, 2017: 14). The key reason comparative case study analysis varies from normal case study analysis is that it seeks to understand how humans and the social structures they created influence specific events or situations. This is critical for this dissertation's research as policy development is led by people and understanding that the processes for creating strategic documents is heavily influenced by ministers' and various departments' key interests as well as the government as a whole.

Comparative case study analysis will be a beneficial method for this research because it looks at cyber incidents as an individual event, as well as an event that contributes to the greater threat landscape which then impacts how the UK, specifically, modifies their national security strategies and policies to engage these threats head-on. Past research into strategy development specific to cyber security is fairly limited because cyber security strategy is fairly new in a political and strategic context. Therefore, there is considerable room for more research to be conducted on how the UK handles these threats to ensure security. This is especially true if they are engaging in adequate pre-emptive approaches to cyber risks, and if the strategies are themselves dynamic enough to immediately respond to new threats that arise. This study will be specific to the UK and their own national cyber security strategies, so it will not necessarily be useful in applying to other nations as threats and abilities vary state to state. I anticipate that many of the conclusions reached in this research will have some applicability and/or utility at an organisational level. This method will be beneficial to gain rich insight into the reasons behind some pervasive and large-scaled cyber-attacks that have happened in the past few years, which remains a gap in research still, as well. This method will help understand common themes between these various cyber-attacks, specifically regarding the human aspects such as who was target, how they were targeted, and why.

To address this, I will examine case studies of past cyber extortion attacks that have occurred in the past ten years. I will examine each event in great detail. The analysis of each case

study will examine what happened in each attack, focusing on who was targeted in the attack (both the intended targets and the secondary victims), how the attack was committed, the scale of the attack, various organisations' response to the attack, and finally, what policies and/or procedures were put in place at a national and organisational level to prevent future exploitation through those vulnerabilities. The case studies chosen will be what John Gerring refers to as 'influential cases', (Gerring, 2007: 108) as these cases have substantially influenced cyber security responses and protocol. They have also created a new baseline for security measures by which nations are beginning to orient themselves.

To conduct the case study research, I will be using primary sources to resolve the research question. The main sources I will utilise in this analysis are published strategic documents, debates and speeches in Parliament or in the news, and quotes from news outlets by ministers, parliament members, etc. (Yin, 2018: 110-117). Principal sources will be useful and crucial elements of this research because I will be able to directly see how strategy has been influenced by large-scale cyber incidents through implementation, discussions regarding legislation, and direct change in strategic documents published during different time periods. The UK government website will be key to obtaining all these sources because everything will be archived and organised for open-access. These documents are necessary in order to better understand how the UK national cyber security strategies have evolved throughout the past decade, and if the documents' development has recognised changing threats in cyberspace and attempt to mitigate those through proactive methods. Policy and strategy analysis will need to be conducted in conjunction with the analysis of the impacts and lessons learned from the specific cyber incidents to allow for a more comprehensive and objective insight into how the UK government is managing a dynamic cyber threat landscape in national security strategies.

3.3 Selected Cyber-Attacks

The attacks this research will be studying are the WannaCry attack from 2017, the NotPetya attack from 2017, and the Stuxnet attack on Iran in 2009. These attacks were some of the largest and most successful ransomware attacks seen thus far, which makes them important to research to gain a better understanding in how to combat ransomware attacks in the future through improved security policies and behaviours.

All the cases mentioned are influential cases. Studying them will help gain better insight into cyber extortion attacks, as attackers could likely take note of them. Possibly utilising the same exploit, using similar tactics to get access to networks, using the same type of malware and/or malware coding, among others. Examining these three cases in-depth will provide the research the opportunity to uncover a variety of possible themes that connects the cases together, as well as provide some diversity of what cyber-attacks might look like.

I have chosen WannaCry and NotPetya because they have happened within the past two years and were unprecedently wide-spread. WannaCry affected a variety of organisations from universities to hospitals to every-day individuals (Symantec Security Response Team, 2017a). It will be interesting to examine how this attack became so pervasive that no organisation or company was necessarily safe from its effects. It will also be important to understand what role cyber strategy and policies played in the exacerbation or mitigation of it. NotPetya followed shortly after WannaCry occurred, but its main 'target' was Ukraine and organisations within the country (Symantec Security Response Team, 2017c). Examining the similarities and differences regarding this attack in its origins, spread, and impact compared to WannaCry, and the other two cases, could help better inform and guide individual behaviours and organisational policies. The third attack that will be used in this case study and strategy analysis is the Stuxnet cyber-attack that targeted Iran and their nuclear development systems. Stuxnet is a crucial event to study as it was considered the first 'cyber weapon' of its kind (Fruhlinger, 2017a). Stuxnet is significant because it was used for state-sponsored sabotage against another state (Fruhlinger, 2017a). This event also preceded the first published UK national cyber security strategy, so it will be important to examine whether the strategy addresses the weaknesses exposed for industrial infrastructure in addition to examining the government's ability to process new strategies based on constantly transpiring and enhanced cyber threats.

3.4 Data Analysis

I will examine the two most recent publications of the official UK cyber security strategy. I will analyse the changes that were made from the first publication to the second one considering strategy, threat landscape, national interests, and the goals for the future. The research will utilise the three specified cyber incidents to further observe how the consequences and lessons learned from those events were either translated into the next strategy or how they have prompted new discussions concerning what needs to be improved or altered for the future.

These discussions could manifest in multiple formats such as new or adjusted definition of threats and threat actors, creation of the new preventive instruments and measures, the creation of new coordinating institutions to manage these issues, and/or new legal arrangements with other UK-based organisations or other nations.

3.4.1 Explanation Building

After organising common themes within each case study and better understanding the processes and outcomes of each them, I will use the explanation building technique to create an explanation for the case studies, also known as process tracing (Yin, 2018: 179). As explanation building is a more specialised form of pattern-matching it will be useful to utilise both to create more in-depth and comprehensive explanations and analyses of the cases. Having the basis of the processes and outcomes of each case study will help to thoroughly develop an explanation for each phenomenon that might drive change to cyber security strategy. It will be difficult to organise and develop causal sequences of each case as for cases like the ones examined in this research did not necessarily progress in a linear fashion and neither does strategy development and implementation; however, it will still be beneficial to examine each narrative to see the commonalities that might have led to alterations in strategic planning which will help contribute to the theories that already exist to examine how the UK is managing dynamic cyber security challenges, and if that is enough to ensure security and resilience.

3.4.1 Cross-Case Synthesis

Another useful analytic tool for this research will be the cross-case synthesis which utilises a 'case-based' approach to multiple case study research (Yin, 2018: 194-196). The goal of case-based analysis is to find within-case patterns for each case study, then compare those patterns to the other cases studied alternative to looking at variables across all cases and matching those (Yin, 2018: 196-197). Conducting a within-case analysis first to draw conclusions about the individual cases and then how they individually have impacted strategy will permit me to examine whether there are theoretical or literal relationships across all the cases (Yin, 2018: 196-197). It is crucial to this analysis to recognise that there will be inherent differences in the cases studied. Therefore, it will be essential to discuss how the cases are comparable along important dimensions such as cultural, institutional, etc. to allow for common findings between them (Yin, 2018: 197-199). This will rely upon making an argumentative interpretation similar to an analytic generalisation that is not reliant upon using quantitative data

to conceptualise the findings (Yin, 2018: 197-199). To properly conduct this analysis, I will need to develop strong, plausible, and fair arguments supported by the data found (Yin, 2018: 197-199). It will also be important to discuss, or at the least, recognise the most plausible rival arguments that could potentially undermine the research and invalidate the findings (Yin, 2018: 197-199).

3.5 Conclusion

Following the analysis of each case's impact on the development and alternations to the UK's cyber security strategy, the next, and most important step will then be to develop conclusions regarding how the UK is able to maintain national resilience in the face of ever-changing threats and new vulnerabilities constantly being discovered. This will be evident by the government's ability to quickly address surprise cyber incidents, mitigate static vulnerabilities that do not improve even after strategy addresses it, and other methods, which could demonstrate if the UK government is successfully utilising cyber strategic culture by sufficiently and effectively, considering historical context from the case studies, various cultures of threat actors and the UK itself.

Chapter 4: Cyber-Attack Cases

4.1 Introduction

The purpose of this section is to describe in detail three significant cyber-attacks that have occurred in the past decade. These attacks will then be utilised in the analysis chapter of this research to determine how the UK's national cyber security strategy has developed and changed in recent publications while taking into account the outcomes and implications these events established. This section will discuss the who, what, when, where, how, and briefly touch upon the why of each cyber incident to give the reader a comprehensive understanding of the specific events. This will help the reader understand why they are important in contributing to the analysis of whether the UK's national cyber security strategy accurately reflects the current threat landscape. It will also address whether those threats are being managed in a proactive manner or if the UK is falling behind the evolution of threats.

4.2 Stuxnet

Stuxnet was first identified in 2010 after infecting an Iranian uranium enrichment plant (Zetter, 2014). It was the first so-called 'cyber weapon' that the international community had come across. It was extremely sophisticated for its time, utilising several unknown Microsoft Windows zero-day exploits (Fruhlinger, 2017). Stuxnet was the first form of malware that was specifically used to conduct cyber espionage by, what was eventually to be determined, as state-sponsored via the United States and Israel (NJCCIC, 2017). Stuxnet is a crucial cyber incident to look at when analysing national cyber strategy development because it was a turning point for the reach of state-sponsored espionage and sabotage, as well as exemplified what damage could be caused by technology and malware. This was one of the first incidents that illustrated the vulnerabilities that existed in both operating systems as well as human security behaviours that needed to be addressed in strategies around the globe to better protect nations' security.

Stuxnet was discovered in June 2010 by a security company based in Belarus after uncovering the worm in computers that belonged to Iranian customers (Strategic Comments, 2011: 1; Elsevier Network Security, 2010: 1-2), though some security researchers believe that the worm had begun to infect Iranian computers from as early as 2007 (Landesman, 2018). According to Symantec, nearly 60 percent of computers affected by the Stuxnet malware were located in Iran (Strategic Comments, 2011: 1). Due to the newness of information security and cyber threats, Iran was unable to detect the malware until after it had caused mass destruction on

their facilities (Strategic Comments, 2011: 1; Farwell and Rohozinski, 2011: 23-25). The ultimate goal of Stuxnet was determined to have been to slow down Iran's ability to create and proliferate nuclear weapons (Fruhlinger, 2017). It specifically targeted the Iranian uranium centrifuges that enriched uranium (Zetter, 2014). The attack resulted in approximately 1,000 centrifuges being damaged and was seen infecting unintended computers in the wild (ICS Malware, 2017).

Stuxnet was extremely damaging to the Iranian facilities it infected and was also sophisticated as it only spread through specific programmable logic controller (PLC) programmes (Farwell and Rohozinski, 2011, p. 23-25). The initial attack vector was initiated via USB removable memory sticks, which once inserted into the targeted computers, would then release the malware (De Falco, 2012: 4-6). It then would self-propagate using either one of four zero-day Microsoft Windows vulnerabilities or STEP 7 (.S7P) files (De Falco, 2012: 4-6). The four zero-day vulnerabilities employed by this malware were as follows:

1. A Windows shortcut 'LNK/PIF' files automatic file execution (De Falco, 2012: 7).
2. Windows print Spooler Service remote code execution (De Falco, 2012: 7).
3. Windows Kernel Win32K.sys keyboard layout privilege escalation (De Falco, 2012: 7).
4. Windows task scheduler privilege escalation (De Falco, 2012: 7).

These four vulnerabilities in Microsoft Windows' operating system allowed the malware to move within a local network without any human interaction (De Falco, 2012: 4-6). To propagate in the infected system, the malware will attempt to gain elevated user privileges and install a rootkit to avoid detection by antivirus software by using forged identification certificates to feign legitimacy and trustworthiness to the system (De Falco, 2012: 5-7). It then initiates its Remote Procedure Call (RPC) server to detect other infected machines in the local network to then communicate with (De Falco, 2012: 6). This is crucial for the malware as the communication allows it to update itself through each other if it cannot connect to the internet and reach the threat actor's command-and-control (C2) server (De Falco, 2012: 6). From here, the malware specifically searches for Siemens WinCC software since that software is used by industrial facilities (De Falco, 2012: 6). It runs through this software folder to find a specific file, where it then renames it, granted the malware access to read, write, and delete code on the PLC (De Falco, 2012: 6). Stuxnet then searches for STEP 7 files which ultimately allows it to upload

attack code into the PLC to modify the system and prevent it from operating properly (De Falco, 2012: 7). This specifically impacted the uranium-enriching centrifuges. The malware was revolutionary for a variety of reasons, including the fact that it had an expiration date for 2012 to desist propagation (Farwell and Rohozinski, 2011: 23), and sent fake data to an operator to pretend that the PLC was functioning properly and appear as though nothing was wrong (De Falco, 2012: 7).

This malware was exceptionally complex and caused mass damage to the Iranian nuclear plant it targeted, which prompted many theories regarding the culprits behind the attack. Attribution of this specific attack is important as it helped inform future strategy and nations that the vulnerabilities cyberspace and technology created could be exploited by state actors for geopolitical gain. The United States and Israel in partnership were eventually attributed with conducting that attack (Nakashima and Warrick, 2012; Lachow, 2011: 118-121). The nations built it as a means of nuclear deterrence against Iran as they both had stake in diminishing Iran's ability to potentially create nuclear weapons (Nakashima and Warrick, 2012; Lachow, 2011: 118-121). The United States being the assumed perpetrator behind that attack meant that it had advanced and aggressive cyber offensive capabilities that could be used on both enemies or allies for political gains. State actors engaging in cyber-attacks created another area that needed to begin to be addressed by nation-states in security strategies to manage national security and mitigate threats. Stuxnet was important for the future of malware, as well, because it showed the utility of Windows' exploits that eventually would be used in the other two attacks discussed in this section.

4.3 WannaCry

The WannaCry outbreak in May 2017, was one of the most damaging attacks that have happened globally, infecting over 300,000 computers in 150 different countries, including 48 United Kingdom National Health Service (NHS) trusts (GOV.UK, 2018). The attack began on Friday, May 12th, 2017 utilising the 'EternalBlue' Microsoft Windows exploit that the hacking group, the Shadow Brokers, made public after stealing it from the United States' National Security Agency (Symantec Security Response Team, 2017a). The first variant of WannaCry was stopped infecting new machines when a security researcher inadvertently activated a kill-switch for the malware and stopped it from further spreading (Vigliarolo, 2017). Other variants

of WannaCry without the domain kill-switch appeared almost immediately after the first kill-switch halted the attack (Newman, 2018). The attack lasted until May 15th.

WannaCry is a form of ransomware, which encrypts a variety of a user's files and then requests money in return for a decryption key. The ransom demands the payment be in the form of cryptocurrency, specifically Bitcoin, because anyone in the world could purchase Bitcoin, allowing for a larger pool of potential victims. If a victim paid out the ransom, in theory, the attackers would then give the victim a decryptor tool to unlock their files (GReAT, 2017). The initial ransom charged $300 USD in Bitcoin, which purportedly would increase to $600 USD if it was not paid within a certain timeframe (GReAT, 2017). Bitcoin is easily traceable compared to other forms of cryptocurrency, like Monero, which might lead threat actors to use those instead in future attacks (Corcoran, 2018). Because the ransom amount was so low compared to what it could have been, it was posited by many researchers that the end-goal of the attack was not financially-driven, but more likely, destruction and chaos were the intended outcomes. The ransomware changed the user's computer background to inform the victim that their files had been encrypted. An application windows displayed the ransom instructions, as well as allowed for the note to be available in 28 different languages and provided a sort of "user manual" in English (GReAT, 2017).

Although the initial attack vector is unknown, the attack vector of how WannaCry self-propagates is well-researched and will be outlined in more detail in this section. WannaCry utilised a vulnerability within Windows Server Message Block (SMB) protocol (Vigliarolo, 2017). The SMB protocol is used for, but not limited to, file sharing between Windows machines on Local Area Networks (LANs). The malware was observed using this protocol to spread within the infected networks because it does not require user interaction to further it (Vigliarolo, 2017; Symantec Security Response Team, 2017a). Once WannaCry infected a machine, the malware would attempt to connect to the domain 'www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com' (Berry et al., 2017). If an IP address was resolved and the malware performed a successful HTTP GET request to the domain, the malware would exit out and not run anything malicious (Berry et al., 2017). By registering the domain and pointing it to a Web server, this check basically acted as a kill-switch for the malware. If the domain was not successfully accessed, the malware would begin to run and

encrypt the files on the machine whilst spreading within the network through the SMB vulnerability (Berry et al., 2017). During this process, the malware would load an embedded RSA public key into the machine creating a thread for moving and deleting files after they were encrypted (Berry et al., 2017). This would then allow for the configuration of the Bitcoin wallet and the 'Ooops, your important files are encrypted' alert to show up on the infected machine (Berry et al., 2017).

During the execution of the malware, following the encryption process, the malware communicates with an Onion server accessed via Tor (The Onion Router) to register the infected machine and transfer the encryption key (Berry et al., 2017). Tor is a tool that allows users to connect to the Internet through virtual tunnels rather than direct connections which circumvents censorship and anonymises access to the Internet, ensuring privacy (www.Torproject.org, 2018). At this point, the malware is able to then communicate with the Tor server to check if a ransom is paid, by clicking the "Check Payment" button. The encrypted private RSA key is sent to the server, which is able to reply with the decrypted private RSA key, so the files are able to be unencrypted (Berry et al., 2017). However, this system had no way for attackers to determine which machines had actually paid the ransom, so even individuals who did pay the ransom did not get their files back due to this flaw (Symantec Security Response Team, 2017a).

In the wake of the attack, it was disclosed that organisations like the UK's National Health Service (NHS) in England, FedEx, Spain's Telefonica, Russian Ministry of Internal Affairs, a major German railway service, telecommunication companies, universities, banks in Ukraine, and many others were those affected by WannaCry (Vigliarolo, 2017). Many organisations that were affected did not publicly disclose the extent of the impact WannaCry had on them, but we can still create lessons learned from the attack, following an examination into how the NHS dealt with the aftermath of the attack, since that has been made public.

80 trusts within the NHS England network and almost 600 General Practitioner practices were infected from WannaCry, causing major disruptions in daily services (Smart, 2018). Between May 12 and 18, over 19,000 appointments were cancelled according to the National Audit Office (Comptroller and Auditor General, 2018). While the NHS had a plan for how to respond to certain incidents, it was never tested at a local level and there was not a plan in place for cyber-specific incidents (Comptroller and Auditor General, 2018). When WannaCry hit, the

NHS had no clear idea of who should lead the response to it and whom to communication with (Comptroller and Auditor General, 2018). A common theme found across many organisations, though particularly apparent in the organisations affected by WannaCry, was that while they had security policies in place, many did not follow their own cyber security policies; it is also possible that security patches were not applied because they could break other applications an organization may use. The patches Microsoft released for the vulnerabilities exploited in this attack were not immediately applied, as well as some organisations utilised unsupported software like Windows XP which Microsoft no longer issues updates or patches for.

Despite many organisations and individuals not getting their files back, the threat actors behind the WannaCry attack made approximately £108,953 in Bitcoin (Gibbs, 2018). Considering over 200,000 machines were infected in the attack, the financial profit the attackers made was comparatively low. This led to a variety of theories generated concerning the actual intention of the attack along with who led the attack. Symantec and other security researchers have ascertained that the attack was most likely to cause chaos rather than make a profit (Symantec Security Response Team, 2017b). Since the attack was not financially-driven, the alternative theory is that it was most likely a state-sponsored attack (Symantec Security Response Team, 2017b). Researchers have determined that it was most likely conducted by a North Korean-linked APT, Lazarus group, because of similarities linking their tactics, techniques, and procedures (TTPs) (Symantec Security Response Team, 2017b; Lord Ahmad, 2017). This is important to keep in mind as during the analysis section of this research, it will examine how the UK national cyber security strategy has addressed (or failed to address) the cyber espionage threats by state-sponsored threat actors. The NHS is supposed to come out with an estimate as to how much the attack cost the department sometime after June 2018 (Donnelly, 2018). However, it has been determined that the government will allocate over £150 million in the next three years to improve the NHS resilience to cyber threats with '£21 million dedicated to address key vulnerabilities in major trauma centres and ambulance trusts' (Hall, 2018) and £39 million allocated to various NHS trusts to address their infrastructure shortcomings (GOV.UK, 2018). These failings in policy and procedures will be examined in more detail in later chapters of this research.

4.4 NotPetya

Shortly after WannaCry occurred, another major cyber incident affected the globe. This new attack transpired in late June 2017, when many organisations and businesses were still working to recover in the aftermath of WannaCry. This attack targeted a majority of Ukraine organisations, specifically Ukraine infrastructure and other major companies, though international companies were also severely impacted (Burgess, 2017; Perez, 2017). Many attribute the attack to Russia, though Russia vehemently denies it was their doing despite recent evidence researchers have released that incriminates Russia (www.bbc.co.uk, 2018).

NotPetya is not the first kind of this specific malware. It was initially believed to originate from a previous version of malware called Petya, which was seen in attacks on Windows-based systems in 2016 (LogRhythm Labs, 2017); however, the malware was determined to have similar binary code to the Petya variant, 'GoldenEye' (LogRhythm Labs, 2017). This malware infected the computer's master-boot record, which prevented the infected machine from starting up properly (Symantec Security Response Team, 2017c). The malware would then load a ransomware notification textbox on the infected machine, where it would inform the user that their system is infected and only fix the system if a ransom was paid to the threat actors in Bitcoin (Symantec Security Response Team, 2017c). NotPetya was initially considered to be a Petya version because they share similar coding; however, as the name suggests, NotPetya is different in a variety of ways. Notably, it was disguised to be ransomware, but actually turned out to be a 'wiper' (Fruhlinger, 2017b). It utilised the same Server Message Block (SMB) exploits that WannaCry used, 'EternalBlue' and 'EternalRomance', to self-propagate, and could spread within the network once infecting one machine even if an organisation patched up their systems because it collected user credentials from the first machine, rendering the need for the SMB exploit unnecessary for further propagation (Symantec Security Response Team, 2017c; Fruhlinger, 2017b; LogRhythm Labs, 2017).

The initial attack vector began through a malicious software update for MEDoc, a type of tax and accounting software that many organisations within Ukraine used (GReAT, 2017b). Networks were notified to update the MEDoc software, and through allowing that "update" to occur, the malware could infect the system (Symantec Security Response Team, 2017c). Once the malware infected one computer, it utilised the user credentials gathered to then spread into other machines in a network (LogRhythm Labs, 2017). The malware creates a list of IP

addresses to spread to within the Local Area Network (LAN) as well as remote IP addresses by collecting credentials through the Windows Credential Manager, and executes a 32bit or 64bit credential dumper (Symantec Security Response Team, Symantec, 2017c). The malware then checks if specific firmware is installed, specifically Kaspersky, Norton Security, and Symantec (LogRhythm Labs, 2017) and uses the "ns.exe" or "ccsvchost.exe" processes, which will determine whether it will utilise the SMB exploits (Symantec Security Response Team, Symantec, 2017c). Once NotPetya is in a system, it will modify the master root record to commandeer the loading process of a system reboot, and schedules a reboot to allow it time to propagate to other machines in a network (Symantec Security Response Team, Symantec, 2017c). This then encrypts 65 types of files on the hard drive like .c source, .pdf, PowerPoint files, Python, VMware images, Excel spreadsheet, amongst several other types of files (Thomson, 2017). A ransom note is then displayed to the user (Symantec Security Response Team, Symantec, 2017c). The ransom note asks for $300 USD in Bitcoin sent to the email address 'wowsmith123456@posteo.net' to receive the decryption key to retrieve the victim's files back (GReAT, 2017b). While the attackers ended up making approximately $6,000 USD in Bitcoin (GReAT, 2017b), the motives behind the attack appears to not have been financially driven (Barth, 2017).

The attack is suspected to have been not financially driven due to the fact that NotPetya was uncovered to act as a wiper, rather than ransomware (Barth, 2017). This specific malware was designed to use a CryptGenRandom function to randomly generate data in the computer (Ivanov and Mamedov, 2017). This meant that instead of the final installation string in the coding contain encrypted info used to restore the decryption key, it just contained random information (Ivanov and Mamedov, 2017). Because of this, users, even if the ransom was paid, could not retrieve their files. This malware ultimately wiped out the information it encrypted (Ivanov and Mamedov, 2017). This 'flaw' in the NotPetya malware suggests, then, that the motive for the attack was to cause destruction and chaos (Barth, 2017). Researchers discovered that approximately 70 to 80 percent of the victims in this attack were in Ukraine, with Ukrainian critical infrastructure, government offices, banks, and nuclear power plants being a handful of the institutions targeted (Barth, 2017; Burgess, 2017; Fox-Brewster, 2017). Other major international institutions were also severely affected by NotPetya, like shipping company Maersk, pharmaceutical company Merck, FedEx, and even some Russian institutions (Burgess,

2017). Many of the organisations affected saw their Ukraine offices infected, which then spread to the rest of their networks (Perlroth et al., 2017). It is estimated that NotPetya caused business at least ten billion USD in damages, if not more (Tehrani, 2017). FedEx-owned company, TNT Express found their Kiev-based office infected with NotPetya, which then infected the rest of their organisation's network (Kovacs, 2017). Interestingly, FedEx was also affected in the WannaCry attack, and while it is unknown how NotPetya infiltrated TNT Express' system, it could be posited that they had yet to patch their operating systems and did not ensure their third-party vendors did, as well.

Some particularly important points to note in the NotPetya attack surround organisational policies and procedures that either were not in place or not enforced which contributed to the severity of the impact it had. This will be important to note for the future chapter which will examine how the UK government specifically has altered their national cyber security strategy in the wake of NotPetya and the common lessons learned from it. One common theme found was that many organisations did not have cyber insurance or anything like that, just in case they found themselves victim to an attack (Kovacs, 2017). Not having cyber insurance also meant that Ukrainian institutions and global organisations not only were without assistance to offset the costs related to the recovery process (Lindros and Tittel, 2016), but also many lost millions of dollars in revenue (O'Connor, 2017). It is important to examine how NotPetya impacted businesses and organisations, even though it did not directly affect the UK's national resilience. This is because some of the common themes surrounding the attack's spread, the repercussions it had, and the lessons learned from it should also influence the continual development of national cyber security strategy. Laying out exactly how these notable cyber-attacks occurred, why they had a negative impact, and the lessons learned by specific organisations will allow this research to then analyse if the UK government examines their own cyber strategies and procedures and alters their national cyber security strategy to account for the dynamic threats, the current vulnerabilities, and if it attempts to take a more proactive stance.

4.5 Theme Analysis of Cases

As mentioned in the methodology chapter of this research, part of the analysis will focus upon finding within-case themes and cross-case themes to then analyse the UK national cyber security strategy's evolution. Here, I will organise both types of revealed from the three cases, so those themes can then be elaborated more on in a later chapter. First this will note the within-

case themes, and then will note themes found across the cases. It is important to note that these themes are by no means exhaustive of all the commonalities shared amongst the cases, but ones that I believe are valuable to note for the upcoming analysis chapter.

4.5.1 Within-Case Themes

Stuxnet

1. The intended targets were the centrifuges within a specific Iranian nuclear-enrichment facility.
2. Exploited several vulnerabilities in Microsoft Windows.
3. Malware would stop spreading and working after infecting the specific machines and had a specified expiration date to completely stop the malware.

WannaCry

1. The unpatched Microsoft Windows SMB vulnerability allowed for extensive propagation of the malware.
2. Bitcoin was used as means of making a profit, though the profit was substantially low compared to the number of machines infected.
3. The malware encrypted files but did not organise the encryption keys to be able to decipher which victims have paid to then give a decryption key to them.
4. There malware was indiscriminate in what machines were targeted.

NotPetya

1. Malware was misconfigured, so the encrypted files could never be salvaged by a decryption key.
2. The majority of affected machines and organisations originated from Ukraine.
3. The malware used Microsoft Windows vulnerabilities to propagate.
4. There were only a few Bitcoin wallets that did not make a large profit compared to the number of machines affected.

4.5.2 Across-Case Themes

1. Microsoft Windows vulnerabilities were exploited in the attacks to infect targets.
2. The attacks are theorised to be state-sponsored.

3. The attacks could have been prevented or the extent of the attacks could have been reduced if employees and organisations adhered to better cyber security practices.

These themes, particularly the across-case themes, noted here will then be useful in the analysis chapter of this research. The analysis will take the themes and compare them to the progression of the UK's cyber security strategy development and evolution to see if and how the UK adapts to past incidents and adopts better strategic practices to improve national resilience.

4.6 Conclusion

This section has detailed three specific cyber incidents that significantly hindered the security of the UK government and other UK-based organisations and exemplified the growing need for improved cyber protections from both an organisational perspective and a national perspective. WannaCry, NotPetya, and Stuxnet illustrate the evolving threats that can be present for national institutions which can jeopardise national security. Stuxnet was the first of its kind as a cyberweapon, utilised by state actors to allow for specific geopolitical gains. The utilisation of USB sticks and unknown vulnerabilities in Microsoft Windows operating systems allowed for future cyber threats to be accomplished in the same manner, with increasing sophistication to maintain relevance and effectiveness. WannaCry and NotPetya used similar means through Windows systems' vulnerabilities to propagate and cause havoc to organisations and countries. These three incidents will be used in this research to examine how the UK, in particular, has further developed their national cyber security strategies by taking into account the vulnerabilities these attacks exploited to help create a more robust and resilient strategy that effectively ensures national security. Utilising cyber strategic culture as the foundation to guide the analysis, I expect to see how and if these events have been translated into future plans or published strategic documents. Cyber strategic culture can inform the UK government if norms and beliefs and historical memory effectively inform strategy. The analysis conducted will attempt to align the specific cyber incidents with the officially published national strategies to establish if and how the UK government is reacting to the evolving threat landscape, if the reaction is quick enough to maintain security whilst mitigating threats, and if the government is attempting to take a proactive stance against future threats by developing strategies that can reduce vulnerabilities and mitigate cyber threat before they occur.

Chapter 5: UK National Cyber Security Strategy

5.1 Introduction

This chapter will examine the past UK national cyber security strategies from the publication of the first strategy in 2010 and the most recent strategy white paper that was created for the year 2016 up until 2021. These two strategic documents have been created and implemented into the larger government national security strategy due to the constantly evolving threats that cyber space have allowed to be exploited by threat actors all over the globe. Following the cyber-attack on Estonian infrastructure in 2007, more nation states realised that there was a necessity for government strategy to include cyber threats and how to mitigate those threats to ensure security and resilience in the face of them. As well, the UK specifically experienced two serious data breaches with one in the HM Revenue & Customs in 2007, and the other in Ministry of Defence in 2008 (Comptroller and Auditor General, 2013:10). This greatly marred the UK government's reputation and exemplified the increasing importance of managing information security and risk (Comptroller and Auditor General, 2013:10). The UK's first official national cyber security strategy was published in 2011 and attempted to plan for cyber threats and attacks whilst developing methods to mitigate them. In 2016, an updated national cyber security strategy was implemented to further expanded upon the 2010 cyber security strategy. The 2016 strategy contained different aims and objectives for achieving national security and cyber resilience. This section is intended to outline both cyber security strategies in detail, so the reader will have a thorough understanding of each strategy. This in-depth understanding will lay the foundation for the next chapter of this dissertation which will analyse how the strategies have evolved. This will take into consideration the specific cyber-attacks discussed in the previous chapter to determine if the UK government is evolving alongside cyber threats to maintain national resilience. This analysis will also consider what sort of approach the government is taking whether it is reactive or proactive.

5.2 2010 National Cyber Security Strategy

5.2.1 Threats to UK

This strategy recognises that people have become increasingly dependent upon the digital world for many facets of life, which also makes individuals and nations more vulnerable to threat actors using cyberspace to compromise data and information (UK Cyber Security Strategy, 2011:

15). The government classifies cyber threats to the UK with the highest priority, or a 'Tier I' threat (UK Cyber Security Strategy, 2011: 15).

A prominent threat to national security mentioned is industrial-level fraud crimes along with identity theft on a grander scale and the exploitation of children via the internet (UK Cyber Security Strategy, 2011: 15). The strategy recognises that threats to the UK are not exclusively contained within their own borders (UK Cyber Security Strategy, 2011: 15). Threat actors can originate from anywhere in the world due to the connectivity the internet allows, which expands the scope of both threat actors and possible targets (UK Cyber Security Strategy, 2011: 15).

This section acknowledges that nation states have increased ability to conduct espionage through cyber space, to spy, gather information and data, spread misinformation, or affect critical infrastructure in order to harm the UK (UK Cyber Security Strategy, 2011: 15). The government, military, businesses, economy, and citizens and their rights are now at greater risk from other nation states exploiting the cyber realm for their own advantage (UK Cyber Security Strategy, 2011: 15). On top of nation states having more capabilities to cyber espionage, terrorists also can utilise the internet and technology to harm the UK. Terrorists now have greater reach to supporters all across the world through the internet, and can spread propaganda, raise money for their cause, communicate more securely, radicalise people on the fringe, and so much more (UK Cyber Security Strategy, 2011: 15). National infrastructure could be in danger not only by nation states, but also now through non-state actors as well. Other non-state actors that threaten the security of the UK are so-called 'hack-tivists' who use the internet to also spread propaganda, garner support, and gain access into government organisations to cause disruption, damage the financial success and/or the reputation of organisations, and gain publicity (which then increases support) (UK Cyber Security Strategy, 2011: 16). This strategy accepts that threat actors can originate anywhere in the world and the anonymous nature of the internet makes attribution of attacks to specific threat actors much more difficult (UK Cyber Security Strategy, 2011: 16).

Not only does this strategy recognise the threats cyberspace creates for the UK government specifically, it also notes that cyber threats to businesses in the UK also threaten the economic success of the country, therefore, measures need to be taken to address those threats, as well. While the threats directly to the government are more political in nature the threats businesses face are more financially-driven with economic motives. The targets with businesses

and organisations within the UK are notably sensitive commercial information and intellectual property (UK Cyber Security Strategy, 2011: 16). Here, threat actors will attempt to mar reputations of organisations and impede revenue gains through targeting computers, phones, and other systems via third-party contractors, employees, and customers (UK Cyber Security Strategy, 2011: 16). Because of cyber-crimes against business would have an extreme impact on the UK's economic growth and stability, cyber threats to businesses are included in this strategy document.

5.2.2 Goals for 2015

The main goal to achieve by 2015 as stated in this strategy document is to 'derive huge economic and social value from a vibrant, resilient, and secure cyberspace, where our actions, guided by our core value of liberty, fairness, transparency, and rule of law enhance prosperity, national security, and a strong society' (UK Cyber Security Strategy, 2011: 8). To meet this goal, this strategic document outlines four objectives the must be achieved in order for the outcome to come to fruition. Those four objectives for the UK are:

1. Tackle cybercrime and become a secure place to conduct business through cyberspace (UK Cyber Security Strategy, 2011: 8).
2. Improve resilience to cyber threats and attacks, as well as improve protection to interests in cyberspace (UK Cyber Security Strategy, 2011: 8).
3. Assist in the development of an open, stable, and vibrant internet which UK citizens can safely use, as well as promotes open societies (UK Cyber Security Strategy, 2011: 8).
4. Gain the knowledge, skills, and capabilities necessary to support and achieve their cyber security objectives (UK Cyber Security Strategy, 2011: 8).

5.2.3 Implementation

The document also outlines what the UK government needs to do to successfully execute the four objectives to attain the stated vision and implement the cyber security strategy. This strategic document discusses the National Cyber Strategy Programme (NCSP) which is a four-year investment plan the government put into place to achieve their strategic objectives from 2011 to 2015 (UK Cyber Security Strategy, 2011: 25). Various departments within the government will have specific roles, particularly the Ministry of Defence and the Government Communications Headquarters (GCHQ), as well as the Home Office, the Cabinet Office, and the

Department for Business, Innovation and Skills (BIS) (UK Cyber Security Strategy, 2011: 25). This four-year plan allocates £650 million in funding specifically to this plan (UK Cyber Security Strategy, 2011: 25). This plan is broken up into six different areas where the funding will be allocated to:

1. Single Intelligence Account to build cross-cutting capabilities, such as information assurance (59% of funding) (The UK Cyber Security Strategy, 2011, p. 25).
2. Home Office to tackle cyber crime (10% of funding) (UK Cyber Security Strategy, 2011: 25).
3. BIS will work with the private sector to improve resilience (2% of funding) (UK Cyber Security Strategy, 2011: 25).
4. The Cabinet Office will coordinate and maintain sights on operational threats (5% of funding) (UK Cyber Security Strategy, 2011: 25). The Ministry of Defence to mainstream cyber into defence strategy and policy (14% of funding) (UK Cyber Security Strategy, 2011: 25).
5. The government ICT to build secure online services (10% of funding) (UK Cyber Security Strategy, 2011: 25).

Not only was a substantial amount of money allocated to various departments within the government to improve cyber security, but a variety of policies, practices, and actions were advocated to successfully implement this strategy as a whole (UK Cyber Security Strategy, 2011: 26-33).

With a laid-out division of funds for the National Cyber Strategy Programme, there are specified priorities that fit into the above categories that are also discussed in more detail in this strategic document (UK Cyber Security Strategy, 2011). The Ministry of Defence is intended to create a Defence Cyber Operations Group which is expected to integrate cyber capabilities across defence infrastructure to create improved tactics, techniques, and procedures to increase security in cyberspace (UK Cyber Security Strategy, 2011: 26-27). The intent is to enrich their current abilities in detecting cyber threats, combating those threats, as well as creating more proactive practices (UK Cyber Security Strategy, 2011: 26-33). The strategy also aims to build an international agreement on how to engage in cyberspace and manage cyber-related

misunderstandings between nation-states and reduce escalation from them (UK Cyber Security Strategy, 2011: 26-28). It is explicitly stated that engagement between the United Nations, the UK, and the Organisation for Security and Cooperation in Europe (OSCE) will be crucial to developing these principles (UK Cyber Security Strategy, 2011: 26-28). A vital aim of this whole document is to reduce the vulnerabilities in the UK's own government systems and infrastructure and improve resilience and security (UK Cyber Security Strategy, 2011: 27-28). A large portion of the UK's critical infrastructure is managed by the private sector, so the Centre for the Protection of National Infrastructure (CPNI) is proposed to work alongside the private organisations to ensure that vulnerabilities in the cyber realm, especially cyber espionage, cyber terrorism, and threats to economic prosperity, are being mitigated thoroughly enough (UK Cyber Security Strategy, 2011: 27-29). There are three particularly noteworthy measures this strategy specifies are necessary to achieve the stated vision for 2015:

1. Encouraging the development of more cyber security professionals since there are not enough cyber security experts in the field when compared to the availability of jobs (UK Cyber Security Strategy, 2011: 29).
2. The creation of the National Crime Agency (NCA) which will aim to broaden law enforcement's capabilities for cyber-crime (amongst others) (UK Cyber Security Strategy, 2011: 29-31).
3. Security awareness and prevention campaigns oriented towards the general public and businesses to improve their security awareness which will therein help protect the UK on a national-level (UK Cyber Security Strategy, 2011: 31-32).

This cyber security strategy underwent at least two separate analyses during the five years it applied to. The National Audit Office and the Cabinet Office examined how the implementation of the strategy was progressing years after it was published to determine the successes and areas for improvement. The reports both found that the allocated funding for specific departments and governmental organisations were being utilised effectively, especially the NCA (Comptroller and Auditor General, 2013; Cabinet Office, 2016). Since a major portion of the strategy focused on funding the new cyber programme, it is a large success that the funds were allocated to the specified departments, and that the creation of certain organisations, like the NCA, have made a massive positive impact on research and further cyber security development (Comptroller and

Auditor General, 2013; Cabinet Office, 2016). The Annual Report from 2016 noted that, whilst progress within the UK is being made to tackle cyber security issues, the threats in cyberspace are only getting more complex and occurring at a higher rate (Cabinet Office, 2016: 30). This means that the UK, at a national and organisational level, need to work harder to match capabilities with the progressing threats.

5.3 2016 National Cyber Security Strategy

5.3.1 Threats and Vulnerabilities

This updated strategy notes that technological change has created more connectivity between countries and people across the globe, including in developing countries, but this change also created a larger landscape for threat actors to engage in (National Cyber Security Strategy, 2016: 17). It also notes that the geopolitical context of the world has also been altered. Nation-states and non-state actors, such as terrorists and activists, are increasingly engaging in demonstrating and experimenting with their cyber offensives where governments are no longer the sole target, but now include the average person (National Cyber Security Strategy, 2016: 17). This section will discuss in more detail the threats and vulnerabilities that this cyber security strategy focuses upon.

Some of the key threat actors this strategy touches upon are the usual suspects: cyber criminals, states or state-sponsored threats, terrorists, hacktivists, and insider threats (National Cyber Security Strategy, 2016: 17-21). The strategy notes that cyber criminals will continue to take advantage of Information and Communication Technology (ICT) devices for fraud, theft, and extortion (National Cyber Security Strategy, 2016: 17-18). The strategy observes that a key threat actor under this umbrella are financially-motivated, Russian-language organised crime groups that utilise advanced malware, specifically ransomware and Distributed-Denial-of-Service (DDoS) attacks, in aggressive manners (National Cyber Security Strategy, 2016: 17-18). Another threat to the UK's security are other states or state-sponsored attacks on the UK. The strategy discusses how cyber espionage and the destruction of UK systems like defence, government, and the finance, telecommunications, and energy sectors are the main goals of these specific actors, and engage in these attacks because they know attribution and legal repercussions are unlikely (National Cyber Security Strategy, 2016: 18-19). While the strategy mentions terrorist as a threat, it is not as emphasised as a high-level threat because terrorists are more likely to continue to focus upon physical terrorism, compared to cyber (National Cyber Security

Strategy, 2016: 19). Hacktivists and 'script kiddies' are mentioned to be probable threats, though they are assumed to be more low-level threats where the intent is defamation or DDoS (National Cyber Security Strategy, 2016: 19-20). One interesting threat that is expanded upon more in the vulnerabilities section, is the insider threat. Insider threats could be either malicious and intentional or unintentional but equally destructive (National Cyber Security Strategy, 2016: 19-20). Malicious insiders have access to sensitive data and information which, if shared with unauthorised person, could cause severe damage to organisations and national security (National Cyber Security Strategy, 2016: 19-20). Equally as dangerous are insider threats that are unintentional, meaning that employees accidentally cause vulnerabilities or infiltration (National Cyber Security Strategy, 2016: 19-20). This will be examined more thoroughly in the vulnerabilities section, as well, because it is specifically is caused by personnel weaknesses.

The main vulnerabilities this strategy highlights are Internet-of-Things (IoT) devices, poor cyber behaviours, lack of cyber security awareness trainings, the utilisation of unsupported or unpatched operating systems, and the ease of access to hacking tools and resources (National Cyber Security Strategy, 2016: 22-23). IoT devices are a great threat to security because they are internet-facing and often connected to other machines in one network. This increases susceptibility for the entire network to be vulnerable to unauthorised access since only one machine needs to be compromised to impact an entire system (National Cyber Security Strategy, 2016: 22-23). As mentioned previously, insider threats can be caused by unintentional behaviour through poor cyber hygiene and habits (National Cyber Security Strategy, 2016: 22-23). This tends to be a result of little to no cyber security awareness training in the workplace (National Cyber Security Strategy 2016-2021, 2016, p. 22-23). Another key vulnerability, especially specific to the UK government and their departments, is the utilisation of unsupported or unpatched operating systems (National Cyber Security Strategy, 2016: 23). The strategy notes this is a problem because exploits used by attackers often target these operating systems that are unprotected, therefore easy to infiltrate (National Cyber Security Strategy, 2016: 23). Lastly, the strategic document discusses that the ease-of-access to hacking tools and resources leaves the UK vulnerable due to the uptake in competent threat actors through the availability of these resources (National Cyber Security Strategy, 2016: 23).

5.3.2 Goals for 2021

This strategy's vision for 2021 is for the UK to be 'secure and resilient to cyber threats, prosperous and confident in the digital world' (National Cyber Security Strategy 2016-2021, 2016, p. 25). To achieve this goal by the end of 2021, the strategy focuses on three key aspects which will allow for the implementation process to be more effectively laid-out and organised under those three separate principles. These key objectives are: defend, deter, and develop (National Cyber Security Strategy 2016-2021, 2016, p. 25). The strategy comments that these can only be accomplished through the interaction and engagement of individuals, businesses and organisations, and the government (National Cyber Security Strategy 2016-2021, 2016, p. 25-29).

5.3.3 Implementation

Defend

To successfully implement this strategy, a major focus of implementation is upon defending the UK and measures that must be taken to ensure security and resilience to cyber threats (National Cyber Security Strategy, 2016: 33-45). Specifically, safeguarding UK networks, data, and systems in the public, commercial and private sectors (National Cyber Security Strategy, 2016: 33). Key policies that are outlined are as follows:

1. The creation of the principle Active Cyber Defence which is meant to impose security measures on all UK cyberspace to strengthen it (National Cyber Security Strategy, 2016: 33-35).
2. Build a more secure internet by developing devices that are pre-installed with security parameters and protocols (National Cyber Security Strategy, 2016: 35-37).
3. Protect the government and its people through the adherence to rigid cyber security standards (National Cyber Security Strategy, 2016: 37-39).
4. Protect national infrastructure and other crucial sectors by providing support that is proportionate to the threats and potential consequences (National Cyber Security Strategy, 2016: 39-42).
5. Improve the public's and businesses behaviours and habits through cyber security awareness and the creation of 'cyber essentials' which all businesses must have to operate (National Cyber Security Strategy, 2016: 42-43).

Through these key goals and objectives, the strategy then anticipates that the UK could be one of the most secure and protected countries in the world.

Deter

The second category that the implementation process must ascertain in this strategy is deterrence, which is applied to both state and non-state actors through a variety of means (National Cyber Security Strategy, 2016: 47-52). The key objectives in this section are:

1. Reduce cyber-crime through the improvement and proliferation of law enforcement capabilities in cyberspace (National Cyber Security Strategy, 2016: 47-49).
2. Form strategies, policies, and practices that proactively and effectively counter hostile foreign actors (National Cyber Security Strategy, 2016: 49-50).
3. Enhance offensive cyber capabilities (National Cyber Security Strategy, 2016: 51).

Through the goals discussed in this section to properly deter cyber threat actors, the strategy can then move onto the third and final stage of the implementation process, which is development.

Develop

Development for the future cyber security capabilities can only occur once the UK is adequately occupied in defence and deterrence. Here, the UK can focus upon long-term goals for development, as it states in the strategy that development must be a twenty-years-plus strategy, rather than simply a five-year-plan (National Cyber Security Strategy, 2016: 55-61). The crucial goals mentioned in this section of the strategy are:

1. Strengthen cyber security skills and foster more cyber security professionals through the coordination between the government, academia, and industry to offer more opportunities in the form of jobs, trainings, and education (National Cyber Security Strategy, 2016: 55-57).
2. Expand the cyber security sector through cultivating the development and support of start-ups (National Cyber Security Strategy, 2016: 57-59).
3. Promote the UK as a leader in cyber security science and technology by building partnerships between universities, research institutes, and government departments to have cutting-edge research (National Cyber Security Strategy, 2016: 59-60).
4. Have rigorous cyber security risk assessments in conjunction with other government risk assessments involving national security and other policy areas to ensure that the threat

landscape is accurately and promptly evaluated (National Cyber Security Strategy, 2016: 60-61).

Creation of the National Cyber Security Centre

The National Cyber Security Centre (NCSC) was created shortly after this document was published in 2016 to encompass all three of the above implementation categories (National Cyber Security Strategy, 2016: 29). It was built to establish a cyber security partnership between the government, industry, and the public (National Cyber Security Strategy, 2016: 29). The NCSC is intended to provide the government, industry, and public with a unified and concentrated source of advice for cyber threats, intelligence, and accessible information (National Cyber Security Strategy, 2016: 29). As a public-facing organisation, it is supposed to generate research and advice on cyber threats, that integrates open-source knowledge alongside GCHQ intelligence and technical experience to create comprehensive analyses for any party (National Cyber Security Strategy, 2016: 29).

5.4 Conclusion

These two cyber security strategies attempt to be comprehensive and up-to-date with the current threat landscape. The initial strategy was the first of its kind to be implemented at a national level for the UK, that was specifically focused upon cyber security. It encompassed the threats and vulnerabilities at the time, while laying the foundation for the creation of multiple institutions within the government and externally, to adequately address all aspects of those vulnerabilities, threats, and countermeasures. It created the NCA and the CPNI to assist in the protection of the country's security. It also gave perspective into how quickly the cyber threats and vulnerabilities for the UK evolved. The second cyber security strategy for 2016 to 2021 noted some key changes to technology and actors that the first strategy did not anticipate. This second strategy aims to make the UK a leader in international cyber security research, as well as a role model for the development and implementation of thorough cyber security policies for the rest of the world. However, as the next chapter will analyse more comprehensively, the UK is struggling to follow through with many of the objectives it intended to achieve in those strategies. The UK is still largely acting reactively to many threats and breaches, also it is not implementing its own recommendations even following major cyber incidents. These points will be discussed in the next chapter.

Chapter 6: Analysis of National Cyber Strategy Evolution

6.1 Introduction

The following analysis utilises the research outlined of the three specific cyber incidents, Stuxnet, WannaCry and NotPetya and specific UK national cyber security strategy documents from previous chapters, to better understand whether the UK's cyber security strategy development and implementation adequately keeps up with the pace of evolving cyber threats or if the UK is falling behind in ensuring national security and cyber resiliency. This will be conducted with the cyber strategic culture paradigm guiding the analysis. This section will analyse the development of the nation's first cyber security strategy and its ability to consider the implications of Stuxnet, then analyse the progress of the second strategy goals following the WannaCry and NotPetya attacks. This section will investigate how the UK utilises cyber strategic culture, specifically historical context and internalisation of new norms and behaviours to improve resilience and ensure security. Consideration will also be given to whether the strategies are proactively addressing key threats in a timely fashion or falling behind in cyber threat prevention.

6.2 Analysis of Cyber Strategy Creation and Development

A year before the first official UK national cyber security strategy was published by the government, the UK published their national security strategy for the years of 2010 to 2015. This document noted that cyber security was becoming a greater problem for the security of the entire nation, though it did take a more terrorism/espionage-orientated stance and perspective regarding cyber security (National Security Strategy, 2010). When cyber-attacks are specifically mentioned in the 2010 National Security Strategy, it notes that the global interconnectivity and the fact that cyberspace is currently seen as a necessity, rather than a privilege, leave the UK government, public, and private sector vulnerable to threat actors (National Security Strategy, 2010: 29-30). This specific document briefly mentions how Stuxnet had a devastating impact on Iran and its infrastructure, which poses as an example of the real-world consequences cyberspace can cause a nation (National Security Strategy, 2010: 29-30). However, as a previous chapter discussed in great detail, Stuxnet could have been prevented through adequate security training since the worm was initiated through infected USB sticks (www.oasistechnology.com, 2014). This strategy notes the implications similar attacks could have upon the UK, yet it does not create any solution or plan on how to use lessons learned from Stuxnet and apply them towards the UK and

it's future. The subsequent first cyber security strategy that was then published in 2011 does not mention Stuxnet or discuss how to adequately combat threats similar to it (UK Cyber Security Strategy, 2011). This leads to the assumption that while the government recognised in the cyber strategy that cyber espionage, sabotage, and nation-states as threat actors are becoming a key threat to national security, the plan proposed is very generalised and not specific enough to effectively prevent similar attacks (UK Cyber Security Strategy, 2011). The National Security Strategy of 2010 does pave the way for the National Cyber Security Strategy to better explain how the UK will maintain and improve security and resilience to cyber threats, but it was still lacking in application and thorough implementation.

Following the publication of the 2011 National Cyber Security Strategy, the National Crime Agency (NCA) was established in 2013, outlined in the plan (UK Cyber Security Strategy, 2011). The NCA was intended to tackle cyber-crime to help combat national-level and primarily domestic cyber-crime (GOV.UK, 2011). The NCA helped the government, private sector, and public become more aware of cyber threats through research, publications, etc., but it was still mostly managing threats reactively as research only uncovered issues and provided the general public with recommendations to avoid specific incidents (Bradley, 2014). Even in her speech MP Karen Bradley notes that improving enforcement capabilities needs to be supplemented by legislative action as well (Bradley, 2014). A scheme called Cyber Essentials was released in 2014, and was intended to form a minimum standard for organisations and industries to have in regards to cyber security (Bradley, 2014). It introduced good cyber security practices for many types of organisations, providing certificates following cyber courses, familiarising employees at all levels with security terminology and basic practices, eventually following its implementation in 2016, GDPR compliance (www.cyberessentials.ncsc.gov).

The first cyber security strategy published did attempt to encompass the threat landscape of the time period and provide solutions to combating the threats it outlined. As the National Audit Office (NAO) noted in their review of the strategy in 2013, the strategy addressed both technical aspects of cyber security, as well as the human aspects of cyber security such as behaviours and attitudes (Comptroller and Auditor General, 2013). A key struggle for the government, as the NAO mentioned, would be getting the government to keep pace with the advancement and sophistication of threats, and adapt rapidly enough to not fall behind them

(Comptroller and Auditor General, 2013: 29-30). This is a critical observation as governments tend to be slow implementing policies and change. Often due to the number and complexity of steps required for approval to move to the implementation stage; additionally, many governmental departments do not actively engage in information sharing or work across departments (Comptroller and Auditor General, 2013: 29-30). This was noted in 2013, and it continues to be a problem still even following the release of the second national cyber security strategy and two major cyber-attacks that occurred within a month of each other in 2017.

The National Audit Office report in 2013 and the Cabinet Office 2015-2016 annual report of the UK cyber security strategy noted that the government had taken a variety of steps to get closer to achieving the goals laid out in the 2011-2016 cyber security strategy. The UK had significantly increased its attention towards cybercrime, and successfully created both the National Crime Agency (NCA) and the Serious Organised Crime Agency (SOCA). These agencies were designed to combat cyber-crime and continue to conduct research on threats and actors (Comptroller and Auditor General, 2013: 19; Cabinet Office, 2016: 12-13). After the damage caused by multiple data breaches and other criminal financially-motivated attacks against various government organisations, the UK government did take that historical context and use it to practically apply the cyber strategy to tackle crime in cyberspace (Comptroller and Auditor General, 2013: 19; Cabinet Office, 2016: 12-13). Police forces began to have trainings on how to combat cyber-crime and then use that training to assist the federal organisations in addressing the issue (Cabinet Office, 2016: 12-13). From a cyber strategic culture perspective, the government was utilising past events and trends to create strategy on how to prevent and address cyber threats in the future. The UK government integrated specific aspects of cyber security practices into law enforcement culture that could then be internalised and further developed in the future. Interesting to point out, however, is that in 2017 following the WannaCry attack, the 2017 National Cyber Security Centre (NCSC) Annual Review of the UK National Cyber Security Strategy mentioned very little in way of solutions to mitigating the impact WannaCry had (National Cyber Security Centre, 2017: 13). WannaCry was initially believed to have been a criminally-motivated attack. The national cyber security strategy should have addressed resolutions to mitigate the effects and better ensure security for the future, but it did not mention anything of this nature (National Cyber Security Centre, 2017: 13). This raises a critical issue that obviously is not being addressed through the actions of the government: they

are not adequately implementing the strategies and plans they have created in the national cyber security strategies to improve national resilience. The NCSC reacted to assist victims and update their guidelines on how to address ransomware (National Cyber Security Centre, 2017: 13), but they did not actually ensure that those recommendations were internalised by both the UK government and other organisations immediately. NotPetya affected similar organisations about a month following WannaCry with analogous attack vectors and propagation. Using cyber strategic culture to analyse whether the UK is able to integrate new habits into their strategic culture based on past events, it is apparent that in this particular case, they are not engaging in the most secure or adaptive behaviours. Cyber security at a national level is crucial to protect citizens and the nation as a whole and requires more than just strategy to ensure security; it requires internalisation and implementation of those strategies and policies.

WannaCry and NotPetya occurred approximately a year following the release of the second strategy. While First Secretary of State Damian Green mentioned that WannaCry and other data breaches highlighted the necessity for organisational action against threats (Green, 2017), he did not suggest that updates be made to the strategy following them or even mention the fact that the NHS, a critical UK government institution, was severely affected due to poor security practices. A key implementation factor in both national cyber strategies was to improve business awareness and establish a bare minimum of cyber security protocol and rules to apply in every organisation, which obviously did not occur. The government did not take their own policy advice from these two strategies, which exemplifies the fact that the government is still slow to adapt to evolving cyber threats. ‘Simple’ cyber security habits like antivirus software and operating system updates were a few tactics that were specifically discussed to be crucial to maintaining security and staying on top of threats (UK Cyber Security Strategy, 2011; National Cyber Security Strategy, 2016), but these simple steps were not employed sufficiently enough as was evident by the severity of the impact and scope of WannaCry and NotPetya.

The NHS Lessons Learned report succeeding WannaCry that was published in February 2018, made a series of recommendations for the NHS and government as a whole with changes to improve security and reduce risk of future breaches. The white paper first laid out the process by which the attack spread, the response the NHS went through after finding out it was infected, and the lessons that the NHS and organisations need to take away from it. One of the key lessons

this report came out with was that the NHS offices affected had not applied the patch to the Microsoft Windows vulnerability (Smart, 2018). The logic behind not applying this patch was that it could negatively impact clinical services depending on how long it would take (Smart, 2018). The offices would have preferred to be vulnerable to unknown risks and threat actors rather than impact their services. This report illuminated key security issues that are still prevalent, despite organisational and national strategy attempting to address them. Here, it has been written into both publications of the national strategy to have improved security behaviours in the government and at an organisational and individual level through various campaigns and awareness programmes; however, security awareness and good cyber security behaviours were still not practiced, which led to WannaCry and NotPetya occurring and propagating. Crucial to the cyber security strategies were that people must engage in better behaviours and security policies need to be more comprehensive, but these were not adopted as part of the developing cyber security culture. This is problematic for ensuring future security and maintaining resilience when almost a decade of strategy specifically mentioning the necessity for security awareness and improved information security management has yet to actually be embraced by the population. The lessons learned from WannaCry are pervasive with the subsequent NotPetya attack, as well as their predecessor, Stuxnet. The issue lies in integrating these lessons into the philosophy of good cyber hygiene to prevent similar future attacks. It is unseen yet if the recommendations made in the WannaCry Lessons Learned report will be implemented, such as creating specific time frames to update operating systems and using software that is still supported by providers (Smart, 2018).

Following the WannaCry attack, the report regarding the investigation into NHS falling victim to the attack determined multiple recommendations to address their vulnerabilities. A few of the recommendations mentioned were:

1. Security awareness training with some trainings oriented for specific roles within the organisation (Smart, 2018).
2. Access to IT systems revoked if an employee does not complete the mandatory security training (Smart, 2018).
3. Improved IT management to mitigate issues (Smart, 2018).
4. Apply system updates immediately after they are released (Smart, 2018).

5. Reduce the level of connectivity within one network so if a system is infiltrated, it cannot infect the full system via an SMB or other vulnerability (Smart, 2018).

Ironically, these recommendations are centred around proper security awareness for employees and organisations. One of the key strategic points in both national cyber security strategies was to implement a minimum standard of appropriate security behaviour for organisations (UK Cyber Security Strategy, 2011; National Cyber Security Strategy, 2016). By mid-year 2017, even critical governmental organisations like the NHS were not adhering to the minimum standard. If the government cannot ensure government-run organisations follow the 'Cyber Essentials' policy, it will be difficult to ensure other organisations implement them properly. This minimises the UK's ability to effectively combat threats. Even simple tasks like updating a machine's operating system should have been an easy task for the NHS so long as it was done in waves, to reduce the impact on services.

Another key problem that was pointed out in the WannaCry incident report was that no clear guidelines exist on how organisations should respond to national cyber incidents. This prompted many affected organisations to report the incident and request assistance in addressing the attack from a diverse assortment of authorities (Smart, 2018: 24). The national cyber security strategies planned to create a national-level CERT which would be the central authority to report cyber incidents to. The national CERT would then organise a response (UK Cyber Security Strategy, 2011; National Cyber Security Strategy, 2016). However, the WannaCry report noted that organisations reported to a variety of authorities, for example: local law enforcement, NHS England, or the NHS Digital (Smart, 2018: 24). This highlights a monumental shortcoming by the government. They did not publicly promote the importance of national CERTs nor did they educate organisations on when CERTs should be notified of a potential cyber incident. This breach in education delayed a sufficient national response to mitigate the attack. The NHS and other organisations affected by WannaCry and other cyber incidents, and the UK government now realise the magnitude of the potential damage caused by not following policies within a strategy.

On top of these deficiencies, the targeted attack on the UK Members of Parliament (MP) and their staff on the 23rd of June 2017 highlighted the government's inability to react quickly to cyber threats, implement changes to their strategies, policies, and behaviours to thwart further

incidents (Guardian Staff, 2017). The email accounts of approximately 90 different MPs and their staff were accessed by threat actors via 'brute force' (Guardian Staff, 2017). The threat actors exploited weak passwords to gain access into email accounts of MPs (Guardian Staff, 2017; National Cyber Security Centre, 2017: 11). Although the goal of the attack is unknown, this shows that even MPs, the people who assisted in creating and implementing the national cyber security strategies, were not following their own guidelines. This could have had severe negative implications for national security had threat actors gained access to documents or items that disclosed classified matters. The UK government should be held to a higher standard of best-practices, especially when it comes to matters of national security; nevertheless, even a month following WannaCry and seven years following Stuxnet, they had not modified their own practices swiftly enough to combat the dynamic and fast-paced threat landscape.

6.3 Conclusion

With such a dynamic cyber risk environment, it is important to recognise that changing strategy and strategic policies is often a slow process. This does make effectively addressing those threats more difficult at a national level. The most obvious challenge the government faces to make amendments to strategy and strategic policies are the fact that policy and strategy development is a process that requires multiple steps and agreement between a number of people at various government levels. Because it is obligatory for policies and strategies implemented at a national level to be vetted before officially put into place, this typically leaves the UK inherently behind threat actors. Even if the government had developed strategic solutions to immediately address the weaknesses from WannaCry, the solutions would not have been executed soon enough to have prevented organisations from falling victim to NotPetya which used the same Microsoft Windows SMB vulnerabilities in the attack. Nonetheless, it does not mean that the government cannot utilise the NCSC, NCA, and other organisations to collaborate to develop pragmatic solutions to cyber problems as they arise. This solution could reduce the severity of a similar future incident before any official strategies are further developed, even when the potential threats are vague, the possible attack vectors are unknown, and the intentions of threat actors are limitless, the risks could still be reduced.

The UK's national cyber security strategies do attempt to be proactive in addressing key cyber threats which is beneficial to national resilience and security. This can be seen through the creation of the NCA, NCSC, and various other departments with emphasis on security awareness

and robust technical security. Yet, it is still very much inherently a reactive strategic plan taking lessons and events from the past to craft its development and implement new practices. However, this does not amend the current strategies as threats evolve and attacks occur. To ensure national security and resilience to threats, the government needs to develop a way that can help streamline particular policies or procedures to get approval expedited through Parliament. Then the government can evolve alongside threats rather than react to them as they occur. This serialised methodology keeps the government and officials a few steps behind, even when the NCSC and NCA are conducting research to try to combat threats and understand the future threat scope. Strategy planning is always going to be a reactionary process because it uses historical context to drive future goals and plans. The UK specifically is taking steps to address recent historical context to help the national cyber culture become more resilient and agile to dynamic cyber threats, but there is still much that can be done to ensure higher levels of security and cyber resilience in a more timely and efficient manner.

Chapter 7: Conclusion

The purpose of this research was to answer that question: how has UK national cyber security strategy evolved to address and ensure national resilience in the face of dynamic cyber security challenges? This analysis went on to systematically outline and explain the significant Stuxnet, WannaCry, and NotPetya cyber-attacks to attempt to correlate those attacks with the evolution of the UK's national cyber security strategy. The investigation of the cyber-attacks was supposed to create historical context and highlight areas for future progression of comprehensive cyber strategy employing the paradigm of cyber strategic culture. Cyber strategic culture was then utilised to study how the UK national cyber security strategy has developed since its first version in 2011 to address the dynamic threats that originate from cyberspace.

7.1 Summary of findings

Here, I will condense and summarise the previous chapters to reiterate the main key points made throughout the research and analysis. As this research has seen, cyber threats are becoming more ubiquitous and frequent which continues to endanger UK national security. The incidents of Stuxnet, WannaCry and NotPetya all occurred with different initial attack vectors, oriented towards different targets, and with different intended goals from the threat actors. Stuxnet was aimed towards Iran's nuclear-enrichment facilities to inhibit their capabilities to create nuclear weapons. It was initiated through malicious USB drives, and exploited several Microsoft Windows vulnerabilities that remained unfixed. It is still unknown by researchers how WannaCry initially began, because it was presumed to have been initiated through a phishing email, though that was later debunked, so researchers are still uncertain how it started. Despite this, it is very apparent that it became so wide-spread because of unpatched vulnerabilities in Microsoft office systems. The ransomware made a moderate profit through the use of Bitcoin, which was also seen in the subsequent NotPetya attack. NotPetya used the same exploits to propagate in Microsoft Windows as WannaCry did, though it was initiated in the Ukraine through a malware-infested MEDoc software update. The cases shared commonalities regarding their propagation through Microsoft Windows' vulnerabilities that were not patched as well as these specific cases were determined to most likely have been conducted by other state-sponsored actors.

The UK cyber security strategies are fairly new, but attempt to be comprehensive in addressing both vulnerabilities as well as means to mitigate those. Key to the strategies were the

allocation of a huge amount of funding directed towards creating new offices and government-run institutions that were intended to address various aspects of cyber security. Military and defence aspects were dealt with by the Ministry of Defence, research and education was left to the newly established institutes: the NCA and the NCSC, and certain aspects of cyber security awareness and training were assigned to the private sector and the general public. It was determined in the analysis section that the UK was trying to implement a variety of different strategies and policies which would generally improve the resilience of the nation towards cyber threats. The strategies were comprehensive as they addressed improvements towards the government's goals and capabilities, public awareness of a basic minimum for good cyber behaviours, research to better understand the threats that exist, future development of more cyber professionals, as well as the adoption of more 'cyber offensive' capabilities rather than relying solely upon defensive capabilities. As the analysis noted, however, the UK was not doing a sufficient job of changing the strategy and making changes as cyber-attacks occurred and threatened security. The strategies were ambitious, but there is still much to be done to ensure national resilience, as the next section will go onto discuss more thoroughly.

7.2 Discussion of Findings

Based on the previous section which amalgamated the information discussed in this entire paper, the answer to the overall research question can be discussed. The UK has been attempting to address the evolving cyber threats since the creation of the first national cyber security strategy through effective and comprehensive strategy. The few versions of this strategy have determined that to best sustain national resilience, the UK must take a multidisciplinary approach. This was seen through the creation of the research institutes: the NCA and the NCSC, as well as new government-run offices developed new responsibilities aimed at cyber security and improving individual security awareness. The strategies allocated an enormous amount of money towards creating these adequate resources, institutions, and cyber-based education programmes that would be dedicated to their overall goal to improve national security, become a leader in cyber security research, and be the most secure place to conduct business in cyberspace. The strategies outlined extremely ambitious goals to attain within five-year time frames in both versions, and while the strategies were fairly specific in the stated methods to achieve their vision, the execution of it all leaves a lot to be desired.

This analysis has discussed in thorough detail the methods and means by which the strategies aim to reinforce national security and resilience, but the execution, as previously stated, has not been sufficient enough to ensure these objectives. Take Stuxnet as an example: it occurred before the first strategy was published and was considered the first 'cyber weapon' of its time. Yet, the implications of Stuxnet regarding the evolution of espionage and the severity of repercussions to an organisation when their information security and systems are compromised was hardly taken into consideration in the strategy. While it did not directly impact the UK, the government could see the impact it had on national infrastructure and utilise those lessons to put towards the nation's own strategy. Even when a major cyber incident, WannaCry specifically, did affect the UK and its own institutions, the cyber security strategy was not amended nor was there a serious Parliamentary discussion on how to nationally fix those weaknesses. On top of that, there has been an overall lack in behavioural changes within organisations and employees to prevent future vulnerabilities through cyber security awareness trainings. Both versions of the cyber security strategy emphasised having a minimum standard of cyber security practices individuals, organisations, and the government should adhere to; however, those were never fully internalised and put into practice. Stuxnet, WannaCry, and NotPetya all could have been prevented or at least the scalability of the attack reduced in some manner through basic security practices like updating operating systems when patches are released to fix vulnerabilities, employees knowing to not connect suspicious USB drives into corporate networks or open links sent from suspicious emails, and having security teams like CSIRTs or SOCs to be the main point of contact for when cyber incidents do arise.

On top of basic security practices needing to be put into practice, the UK government and the national cyber security strategies need to be amended as events occur. The government is slow to adapt and change based on new incidents, which is understandable to a degree because there is a strict process that must be followed to propose and implement those changes. Nevertheless, if the UK wants to be a secure place for institutions and businesses and maintain security, they have to be more active in facilitating alterations to strategy and its policy quicker. This can be seen in the recommendations and lessons learned from the third-party investigation into WannaCry's impact on the NHS. Many of the recommendations from this report still have yet to be implemented, despite its publication in February 2018 and now being on the downside

of 2018. That is extremely problematic since basically it means the UK is not practicing what it preaches and is, therefore, jeopardising security.

It is worth noting that threat actors will inherently continue to be at an advantage compared to nations. Threat actors just need to find one vulnerability in order to inflict damage on a target, while nations and other targets have to preserve security 100 percent of the time. Threat actors have the luxury of time and lack of hurdles to jump through to constantly develop and refine their attack methods, and there are a multitude of actors out in the world who all have a variety of reasons behind their attacks. This means that no one nation is truly fully secure to these threats since they can come through a number of manners. The UK is inherently at a disadvantage compared to threat actors and most likely never be able to create and implement completely proactive strategy against these sorts of threats; however, the recent strategies have, on paper, done a decent job at attempting to mitigate threats and preserve security and become more resilient. Saying that, the UK is still lacking in appropriate and thorough execution of their proposed strategies and strategic policies to attain national resilience and security. There have been strides in the right direction to achieve that goal, but until the national strategy contextualises past events, inputs those lessons into practice, and can develop at a faster pace, the UK will not be able to be resilient in cyberspace.

7.3 Limitations

While this research aimed to be comprehensive in the analysis of the UK's national cyber security strategy and its development throughout the past ten years by utilising specific cyber incidents, there were limitations to the research. The first most prevalent limitation was that the UK's national cyber security strategy has only had two official publications, with the first publication of it distributed in 2011. The relatively contemporary nature of the strategic documents means that the internalisation of the newly proposed norms has yet to fully be embraced. This means that, from a cyber strategic culture perspective, the behavioural aspects of the cyber security strategies have yet to become second nature in practice. Once more basic practices of cyber security become normalised at both an individual level and national level, there might be improvements in the UK's ability to maintain resilience and security. As well, cyber security strategy has not fully been adapted into the general national security strategy since it is still a newly necessary mode of security strategy, therefore it may be of utility to re-examine it in a few years' time when there are more publications of it to properly analyse how the UK is

faring in the maintenance of their national cyber resilience. Another limitation this research faced was that, as a citizen of a different country, I am not well-versed in the processes or the nuances that play into strategy development or implementation in Parliament. Because of this, I may be unintentionally biased in how I conducted the analysis of my research based on my own understandings of how strategy is developed and changed from the perspective of a United States citizen. The interests of the US versus the UK are also different when it comes to national security and resilience, so my understanding of how those should look may also have skewed the analysis, though it does not negate the findings. A final limitation this research faced was the access to resources. The research could have had greater impact had it had the access to discuss the strategy and the impacts of the three specific cyber incidents with institutions like the NCSC, Government Communications Headquarters (GCHQ), or specific MPs who headed the strategy. These limitations, however, can be addressed in the next section regarding future research.

7.4 Future Research

There are a variety of ways this research could be expanded upon in the future, both based on the mentioned limitations and others. Future research could take a multitude of different approaches to further examine the UK's approach to national resilience and security in the face of a dynamic cyber threat landscape. Firstly, future research could wait for a few more official publications of the national cyber security strategy to gain a more comprehensive perspective, utilising cyber strategic culture as the guiding paradigm, into how the UK address dynamic cyber threats and if that is actively observed in strategy and in practice. This research has also paved the way for future research to examine other cyber incidents that may have only been targeted within the UK or incidents specifically against the government, whether successful or not, to better determine how the UK national strategy ensures resilience and security. This may mean that future research could possibly be conducted internally within the UK government as it may deal with cyber breaches within government departments that are not public knowledge. This would also allow for greater input from sources like GCHQ, MPs, the Cabinet Office regarding the specifics of strategy development and implementation based on those breaches and based on a more nuanced understanding of the processes and struggles with national strategy. Another direction for future research could be to compare and contrast national cyber security strategy between nations in order to better understand the failings and successes of the strategies to ensure security. This would allow for a more comprehensive outlook on how

various nations address the dynamic cyber threat landscape within their strategies and actions, which would then allow for nations to learn off each other based on the findings. Understanding where one nation went right in strategy versus another would allow for more comprehensive future cyber security strategy that better ensures protection against the full spectrum of cyber threat actors.

Bibliography

(2010) 'Stuxnet May Be the Work of State-backed Hackers', Elsevier Network Security Newsletter, pp. 1-2

(2011) 'Stuxnet: targeting Iran's nuclear programme', Strategic Comments, pp. 1-3

(2014). 'How to Prevent Stuxnet and Similar Attacks on your Business', Oasis Technology, Available at: http://www.oasistechnology.com/how-to-prevent-stuxnet/ [Accessed 07 July 2018]

(2017) 'Internet Security Threat Report 2017', Norton Symantec Inc

(2017) 'NotPetya Technical Analysis', LogRhythm Labs

(2017) 'About', Cyber Essentials, Available at: https://www.cyberessentials.ncsc.gov.uk/about.html [Accessed 20 June 2018]

(2018) 'Tor Project: Overview', Torproject.org. Available at: https://www.torproject.org/about/overview.html.en [Accessed 10 July 2018]

(2018). 'What is Social Engineering? Examples and Prevention Tips', Webroot, Available at: https://www.webroot.com/us/en/resources/tips-articles/what-is-social-engineering [Accessed 3 Jan. 2018]

'Understanding the relationship between human behavior and susceptibility to cyber attacks: A data-driven approach', ACM Transactions on Intelligent Systems and Technology, pp. 51:1-51:25

'What is a DDoS Attack?', *Digital Attack Map*, Available at: http://www.digitalattackmap.com/understanding-ddos/ [accessed 27 June 2017]

Abawajy, J. (2014) 'User preference of cyber security awareness delivery methods', Behaviour & Information Technology, pp. 237-248

Abendan II, O.C.A. (2013) 'Watering Hole 101- Threat Encyclopedia', *Trend Micro USA,* Available at: https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/137/watering-hole-101 [Accessed 01 July 2018]

Alberts, C., Dorofee, A., Killcrece, G., Ruefle, R., & Zajicek, M. (2004) Defining Incident Management Processes for CSIRTs: A Work in Progress, Pittsburgh: Software Engineering Institute, Carnegie Mellon University

Al-Rodhan, N. (2015) 'Strategic Culture and Pragmatic National Interest', Global Policy, pp. 1-4

Armerding, T. (2018) 'The 17 biggest data breaches of the 21st century', CSO Online. Available at: https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html [Accessed 28 June 2018]

Barth, B. (2017) 'Key researchers reclassify NotPetya as a wiper, suspect destruction was true motive', SC Media US, Available at: https://www.scmagazine.com/key-researchers-reclassify-notpetya-as-a-wiper-suspect-destruction-was-true-motive/article/671940/ [Accessed 26 June 2018]

Bartlett, L. and Vavrus, F. (2017) 'Comparative Case Studies: An Innovative Approach', Nordic Journal of Comparative and International Education, pp. 5-17

BBC News. (2018) 'Russia blamed for 'malicious' cyber-attack', BBC, Available at: https://www.bbc.co.uk/news/uk-politics-43062113 [Accessed 24 Jul. 2018]

Beautement, A, Becker, I., Parkin, S., Krol, K., and Sasse, A. (2016) 'Productive Security: A Scalable Methodology for Analysing Employee Security Behaviours', in Twelfth Symposium on Usable Privacy and Security 2016, USENIX Association, pp. 253–270

Ben-Asher, N. & Gonzalez, C. (2015) 'Effects of cyber security knowledge on attack detection', Computers in Human Behavior, pp. 51-61

Berry, A., Homan, J., and Eitzman, R. (2017) 'WannaCry Malware Profile', FireEye, Available at: https://www.fireeye.com/blog/threat-research/2017/05/wannacry-malware-profile.html [Accessed 10 July 2018]

Booth, K. (2007) Theory of World Security, Cambridge: Cambridge University Press

Bowen, B.M., Devarajan, R., and Stolfo, S. (2011) 'Measuring the Human Factor of Cyber Security', IEEE International Conference on Technologies for Homeland Security (HST), pp. 230-235

Bradley, K. (2014) *UK Cyber Security*, 16 June, IA14 Conference, London

Burgess, M. (2017) 'What is the Petya ransomware spreading across Europe?', WIRED.co.uk, Available at: https://www.wired.co.uk/article/petya-malware-ransomware-attack-outbreak-june-2017 [Accessed 24 June 2018]

Cabinet Office. (2016) 'The UK Cyber Security Strategy 2011-2016 Annual Report', Cabinet Office, London: HM Government

Comptroller and Auditor General. (2013) 'The UK cyber security strategy: Landscape review', House of Commons, London: National Audit Office

Comptroller and Auditor General. (2018) 'Investigation: WannaCry Cyber Attack and the NHS', The Department of Health, London: National Audit Office

Connolly, L.Y., Lang, M., Gathegi, J., Tygar, D.J. (2017) 'Organisational culture, procedural countermeasures, and employee security behaviour: A qualitative study', Information & Computer Security, pp.118-136

Corcoran, K. (2018) 'Law enforcement has a massive problem with these 3 cryptocurrencies', Business Insider. Available at: http://uk.businessinsider.com/law-enforcement-problems-with-monero-zcash-dash-cryptocurrencies-2018-2 [Accessed 07 July 2018]

De Falco, M. (2012) 'Stuxnet Facts Report: A Technical and Strategic Analysis', NATO Cooperative Cyber Defence Centre of Excellence

Donnelly, C. (2018), 'PAC Sets June 2018 Deadline For Department Of Health To Count NHS Cost Of Wannacry', Computer Weekly, Available at: https://www.computerweekly.com/news/252439314/PAC-sets-June-2018-deadline-for-Department-of-Health-to-count-NHS-cost-of-WannaCry [Accessed 03 July 2018]

Duračinská, Z. 2017, *Lecture 4: Organisational and operational aspects of CSIRTs*, lecture notes, Cyber Security and International Relations JPM611, Charles University Prague, delivered 30 October 2017

Farwell, J.P. and Rohozinski, R. (2011) 'Stuxnet and the Future of Cyber War', Survival, pp. 23-40

Fox-Brewster, T. (2017) 'Petya Or NotPetya: Why The Latest Ransomware Is Deadlier Than WannaCry', Forbes, Available at: https://www.forbes.com/sites/thomasbrewster/2017/06/27/petya-notpetya-ransomware-is-more-powerful-than-wannacry/#181b88bb532e [Accessed 23 June 2018]

Fruhlinger, J. (2017a) 'What is Stuxnet, who created it and how does it work?', CSO Online, Available at: https://www.csoonline.com/article/3218104/malware/what-is-stuxnet-who-created-it-and-how-does-it-work.html [Accessed 28 June 2018]

Fruhlinger, J. (2017b) 'Petya ransomware and NotPetya malware: What you need to know now', CSO Online, Available at: https://www.csoonline.com/article/3233210/ransomware/petya-ransomware-and-notpetya-malware-what-you-need-to-know-now.html [Accessed 29 June 2018]

Geers, K. (2011) Strategic Cyber Security, Tallinn: NATO Cooperative Cyber Defence Centre of Excellence

Gerring, J. (2007) Case Study Research: Principles and Practices, Cambridge; New York City: Cambridge University Press

Gibbs, S. (2018) 'Wannacry: Hackers Withdraw £108,000 Of Bitcoin Ransom', *The Guardian*.com, Available at: https://www.theguardian.com/technology/2017/aug/03/wannacry-hackers-withdraw-108000-pounds-bitcoin-ransom [Accessed 01 July 2018]

GOV.UK. (2011) 'New strategy to tackle cyber-crime published', Available at: https://www.gov.uk/government/news/new-strategy-to-tackle-cyber-crime-published [Accessed 23 June 2018]

GOV.UK. (2018) 'Plans to Strengthen NHS Cyber Security Announced', Available at: https://www.gov.uk/government/news/plans-to-strengthen-nhs-cyber-security-announced [Accessed 03 July 2018]

Gray, C.S. (1986) Nuclear Strategy and National Style

GReAT: Global Research and Analysis Team. (2017a) 'Wannacry Ransomware Used In Widespread Attacks All Over The World', SecureList, Available at: https://securelist.com/wannacry-ransomware-used-in-widespread-attacks-all-over-the-world/78351/ [Accessed 19 June 2018]

GReAT: Global Research and Analysis Team. (2017b) 'Schroedinger's Pet(ya)', SecureList, Available at: https://securelist.com/schroedingers-petya/78870/ [Accessed 29 June 2018]

Green, D. (2017) *First anniversary of the National Cyber Security Strategy*, 18 October, NCC Group Headquarters, Manchester

Guardian Staff. (2017) 'Cyber-attack on parliament leaves MPs unable to access emails', The Guardian, Available at: https://www.theguardian.com/politics/2017/jun/24/cyber-attack-parliament-email-access [Accessed 16 July 2018]

Hall, K. (2018) 'NHS Given A Lashing For Lack Of Action Plan One Year Since Wannacry', The Register, Available at: https://www.theregister.co.uk/2018/04/18/mps_slam_nhs_for_lack_of_action_plan_one_year_on_from_wannacry/ [Accessed 03 July 2018]

Hall, M. (2016) 'Why people are key to cyber-security', Network Security, pp.9-10

HM Government. (2010) 'A Strong Britain in an Age of Uncertainty: National Security Strategy', HM Government, London: The Crown

Holt, T.J, Freilich, J.D., and Chermak, S.M. (2017) 'Exploring the Subculture of Ideologically Motivated Cyber-Attackers', Journal of Contemporary Criminal Justice, pp. 212-233

Ivanov, A. and Mamedov, O. (2017) 'ExPetr/Petya/NotPetya is a Wiper, Not Ransomware', SecureList, Available at: https://securelist.com/expetrpetyanotpetya-is-a-wiper-not-ransomware/78902/ [Accessed 23 June 2018]

Johnston, A.I. (1995) 'Thinking about Strategic Culture', International Security, pp. 33-64

Kearney, W.D. and Kruger, H.A. (2016) 'Can perceptual differences account for enigmatic information security behaviour in an organisation?', Computers & Security, pp. 46-58

Kovacs, E. (2018) 'NotPetya Attack Costs Big Companies Millions', SecurityWeek.com, Available at: https://www.securityweek.com/notpetya-attack-costs-big-companies-millions [Accessed 25 June 2018]

Lachow, I. (2011) 'The Stuxnet Enigma: Implications for the Future of Cybersecurity', Georgetown Journal of International Affairs, pp. 118-126

Landesman, M. (2018) 'What Is the Stuxnet Worm Computer Virus?', Lifewire, Available at: https://www.lifewire.com/stuxnet-worm-computer-virus-153570 [Accessed 28 June 2018]

Lindros, K. and Tittel, E. (2016) 'What is cyber insurance and why you need it', CIO, Available at: https://www.cio.com/article/3065655/cyber-attacks-espionage/what-is-cyber-insurance-and-why-you-need-it.html [Accessed 27 June 2018]

Longhurst, K. (2000) 'Strategic Culture: The Key to Understanding German Security Policy?', University of Birmingham

Lord Ahmad. (2017) 'Foreign Office Minister condemns North Korean actor for WannaCry attacks', GOV.UK, Available at: https://www.gov.uk/government/news/foreign-office-minister-condemns-north-korean-actor-for-wannacry-attacks [Accessed 02 June 2018]

Margaras, V. (2004) 'Strategic Culture: A Reliable Tool of Analysis for EU Security Developments?', unpublished conference paper, European Foreign Policy Conference, London

Morgenthau, H.J. (1978) Politics Among Nations: The Struggle for Power and Peace, New York: Alfred A. Knopf, pp. 4-15

Nakashima, E. and Warrick, J. (2018) 'Stuxnet was work of U.S. and Israeli experts, officials say', The Washington Post, Available at: https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html?noredirect=on&utm_term=.3ca8b3aad21c [Accessed 29 June 2018]

National Cyber Security Centre. (2017) 'Annual Review', National Cyber Security Centre, London: HM Government

Newman, L. (2018) 'How An Accidental 'Kill Switch' Slowed Friday's Massive Ransomware Attack', WIRED.com, Available at: https://www.wired.com/2017/05/accidental-kill-switch-slowed-fridays-massive-ransomware-attack/ [Accessed 20 June 2018]

NJCCIC. (2017) 'Stuxnet', New Jersey Cybersecurity & Communications Integration Cell Available at: https://www.cyber.nj.gov/threat-profiles/ics-malware-variants/stuxnet [Accessed 24 Jul. 2018]

O'Connor, F. (2017) 'NotPetya still roils company's finances, costing organizations $1.2 billion in revenue', Cybereason.com, Available at: https://www.cybereason.com/blog/notpetya-costs-companies-1.2-billion-in-revenue [Accessed 24 Jul. 2018]

Orojloo, H. and Azgomi, M.A. (2016) 'Predicting the behavior of attackers and the consequences of attacks against cyber-physical systems', Security and Communication Networks, pp. 6111-6136

Ovelgönne, M., Dumitras, T., Prakash, B.A., Subrahmanian, V.S., and Wang, B. 2017.

Perez, Roi. (2017) 'NotPetya Ransomware: Lessons Learned', InfoSecurity Magazine, Available at: https://www.infosecurity-magazine.com/magazine-features/notpetya-ransomware-lessons-learned/ [Accessed 29 June 2018]

Perlroth, N., Scott, M., and Frenkel, S. (2017) 'Cyberattack Hits Ukraine Then Spreads Internationally', The New York Times, Available at: https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html [Accessed 23 June 2018]

Pfleeger, S.L. & Caputo, D.D. (2012) 'Leveraging behavioral science to mitigate cyber security risk', Computers & Security, pp. 597-611

Protectimus Solutions. (2017) 'The Petya Virus: How It All Went', Protectimus Solutions Available at: https://www.protectimus.com/blog/notpetya-virus/ [Accessed 16 Nov 2017]

Sharot, T. (2011) '*The optimism bias*', Current Biology, pp. R941-R945

Smart, W. (2018) 'Lessons Learned Review of The WannaCry Ransomware Cyber Attack', Office for Health and Social Care, London: HM Government

Sulkoswki, A.J. (2007) 'Cyber-Extortion: Duties and Liabilities Related to the Elephant in the Server Room', University of Illinois Journal of Law, Technology & Policy, pp. 22

Symantec Security Response Team. (2017a) 'What You Need To Know About The WannaCry Ransomware', Symantec Security Response, Available at: https://www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attack [Accessed 19 June 2018]

Symantec Security Response Team. (2017b) 'Wannacry: Ransomware Attacks Show Strong Links To Lazarus Group', Symantec Security Response, Available at: https://www.symantec.com/connect/blogs/wannacry-ransomware-attacks-show-strong-links-lazarus-group [Accessed 01 July 2018]

Symantec Security Response Team. (2017c) 'Petya ransomware outbreak: Here's what you need to know', Symantec Security Response, Available at: https://www.symantec.com/blogs/threat-intelligence/petya-ransomware-wiper [Accessed 24 June 2018]

Tehrani, R. (2017) 'NotPetya: World's First $10 Billion Malware', Apex Technology Services, Available at: https://www.apextechservices.com/topics/articles/435235-notpetya-worlds-first-10-billion-malware.htm [Accessed 25 June 2018]

The Cabinet Office. (2011) 'The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world', The Cabinet Office, London: HM Government

The Cabinet Office. (2016) 'National Cyber Security Strategy 2016-2021', The Cabinet Office, London: HM Government

Thomson, I. (2017) 'Everything you need to know about the Petya, er, NotPetya nasty trashing PCs worldwide', The Register, Available at: https://www.theregister.co.uk/2017/06/28/petya_notpetya_ransomware/?page=3 [Accessed 22 June 2018]

Vigliarolo, B. (2017) 'Wannacry: A Cheat Sheet For Professionals', Techrepublic, Available at: https://www.techrepublic.com/article/wannacry-the-smart-persons-guide/ [Accessed 20 June 2018]

Wada, F., Longe, O. and Danquah, P. (1970) 'Action speaks louder than words-understanding cyber-criminal behavior using criminological theories', The Journal of Internet Banking and Commerce, pp. 1-12

Waldrop, M.M. (2016), 'How to Hack the Hackers: The Human Side of Cybercrime', Nature, pp. 164-167

Yin, R. (2018) Case Study Research and Applications: Design and Methods, Los Angeles: SAGE

Zetter, K. (2014) 'An Unprecedented Look at Stuxnet, the World's First Digital Weapon', WIRED.com, Available at: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/ [Accessed 28 June 2018]