Cybersecurity:

Evaluation of Ireland's efforts to combat Cyber Crime in comparison to other countries

---

Jennifer Inglis O'Brien

A dissertation submitted to the University of Dublin

in partial fulfilment of the requirements for the degree

of MSc in Management of information Systems

29th May, 2019

Declaration

I declare that the work described in this dissertation is, except where otherwise stated, entirely my own work, and has not been submitted as an exercise for a degree at this or any other university. I further declare that this research has been carried out in full compliance with the ethical research requirements of the School of Computer Science and Statistics.

Signed: _____
Jenny Inglis O'Brien

29th May, 2019

Permission to lend and/or copy

I agree that the School of Computer Science and Statistics, Trinity College may lend or copy this dissertation upon request.

Signed: _____

Jenny Inglis O'Brien

29th May, 2019

Abstract

Cyberspace is undisputedly one of the most significant developments in modern history, continuously expanding to impact all aspects of modern human life from both a socio, economic and political aspect. The internet provides a platform in connecting the world and its growth continues at a phenomenal rate. Emerging technologies such as the Internet of Things is expanding the number of devices we connect to the internet, blurring the lines of the physical and cyber world. Critical services such as; energy, transport and banking are also connected to the internet, thus increasing the need for strong resilience to protect against threat vectors and adversaries. The threat landscape and threat actors is continuously changing, from cyber criminals hacking for financial gain to highly sophisticated attacks from suspected nation states in acts of cyber war for political reasons. Cyber-attacks such as the 2007 Estonian attack were the states online services; banking, news agents, governmental websites were inaccessible, Stuxnet; a targeted attack on the Natanz Iranian nuclear plant to halt its nuclear activities and the Ukrainian Power outage attack in 2015 resulting in homes without power for weeks are all examples of attacks on critical services that have gained the attention of major international organizations to respond to the increasing threats on cybersecurity. The European Union and NATO are actively responding with legislations and policies in efforts to make cyberspace safer and respond to threats. The 2013 EU cyber security strategy, the Network and Information Directive and the revised data protection act are such examples of the EU's response.

The research study assesses the threats of cyber space and the responses by international organisations. The research study examines and collates cybersecurity efforts of a selection of pre-determined countries by reviewing each nations National Cyber Security Strategy. The purpose is to compare to Ireland with the results concluding to answer our research questions.

Acknowledgements

Firstly, I would like to thank my supervisor Nina Bresnihan for the advice and continued support over the past year.
I would like to acknowledge and thank, my family, husband Mark for his constant love, patience and ability to motivate me during difficult times. For providing a home environment to make this dissertation completion possible. I would like to thank my children, Ellie and Ciaran.

I would like to dedicate this dissertation to family, especially our new born son Ciaran who was born prematurely on the 22nd April 2019.

I would like to express my sincere gratitude to Paul Walsh who recommended this academic journey and believed in my ability.
Finally, I would like to thank my good friend Aine Andrews for her continuous encouragement and support throughout.

List of Abbreviations

ICT	Information Communications Technology
IOT	Internet of Things
NIS	Network Information Systems
EU	European Union
NATO	North Atlantic Treaty Organisation
UN	United Nations
ENISA	European Network Information Systems Agency
NCSS	National Cyber Security Strategy
CSDP	Common Security and Defence Policy (CSDP)
ISP	Internet Service Provider
CSIRT	Computer Security Incident Response Team
DCCAE	Department of Communications, Climate Action and Energy
GDPR	General Data Protection Regulation

Table of Contents

Chapter One: Introduction

1.1 Background/Purpose of Study

ICT is firmly embedded in our society, widely used to conduct all forms of business and communications. ICT is paramount for businesses and users from transactions as e-economies grow to engaging socially via email and social media platforms. Society and economies have become and are continuing to be increasingly reliant on Information Communication Technologies (ICT). The move to a digital society is exposing organisations, businesses, governments and society to cybercrimes as criminals move digital too. The advances in ICT continues to connect people with emerging technologies such as The Internet of Things (IoT) entering the marketplace at a fast pace and supporting technologies such as quantum computing and artificial intelligence enabling increased connectivity. These developments are further increasing our reliance on ICT.

The Internet of Things (IoT) has drastically contributed to the many devices we now connect online. IOT is now responsible for billions of devices connected to the internet from fridge freezers, home heating, and personal fitness devices to home surveillance cameras of our properties all connected over the internet. All this information is streamed from our devices adding to the number of devices we now connect to the internet. (Statista, 2018), predict by 2020, the number of connected devices (Internet of Things; IOT) worldwide is forecasted to grow to almost 31 billion worldwide. IoT devices bring great convenience but pose many risks to personal security. If not adequately protected, users are potentially inviting criminals into our personal lives and homes.

The lines between the physical and cyber world continue to blur as we move further to digital societies. Another advancement in ICT is the connection of critical services such as water supply, energy and transport that are also connected online. "The expansion of the Internet beyond computers and mobile phones into other cyber-physical or 'smart' systems are extending the threat of remote exploitation to a whole host of new technologies. Systems and technologies that underpin our daily lives – such as power grids, air traffic control systems, satellites, medical technologies, industrial plants and traffic lights – are connected to the Internet and, therefore, potentially vulnerable to interference." (GOV.UK, 2016).

Nevertheless, the threats posed by cyberspace do not outweigh the advantages the internet provides. "An open and free cyberspace has promoted political and social inclusion

worldwide; it has broken down barriers between countries, communities and citizens, allowing interaction and sharing of information and ideas across the globe; it has provided a forum for freedom of expression and exercise of fundamental rights, and empowered people in their quest for democratic and more just societies.” (European Commission , 2018, p. 2). however, the increased sophistication and potential damage of cyber-attacks, possible physical has prompted world leaders and organisations to respond to Cybercrime and review cyber security policies. National governments are now taken active steps to secure the internet while also cognisant of the many advantages of the digital world. Nations continue to strive for digital economies to seek the rewards of digital economies, acknowledging cyberspace for wealth and prosperity.

The purpose of the study is to measure and evaluate Ireland’s cybersecurity preparedness in comparison to other countries and consequently, where applicable, provide recommendations to strengthen Ireland's strategic direction and assist in the development of a new national cybersecurity strategy.

1.2 Research Aims

The overall aim of this dissertation is to assess Ireland's approach to cybersecurity and to evaluate in comparison to other countries if Ireland is doing enough to protect the nations information and communication technologies. By answering the below research questions, the study aims to evaluate current cybersecurity measures.

- Measure and evaluate Ireland’s cybersecurity preparedness in comparison to other countries.
- What are the advanced trends in cybercrimes and subsequent undertakings globally to combat cyber threats?
- What cybersecurity measures has Ireland taken and what foundations are in place to protect the nation?
- Is Ireland doing enough to respond and protect the nation from cyber threats and possible attacks.

1.3 Research Methodology

The analysis will be conducted by reviewing and comparing the national cybersecurity strategies, the main policy document for countries to set out their plans on cybersecurity measures such as objectives and visions. Through analysis of national strategies and comparing Ireland's endeavours will allow us to determine if Ireland is doing enough to respond and protect the nation from cyber threats and possible attacks.

The research methodology and approach for this study involved a combination of methods and followed a mixed methodology approach. The research predominantly employed framework analysis. Two existing frameworks, used previously for analysis of national cybersecurity strategies, were reused to examine new data for the purpose of our research (Luiijf, 2013) (ENISA, 2019). **“**Secondary research involves re-analysing, interpreting, or reviewing past data” (Oxbridge Essays, 2017)**.** The secondary data provided a comprehensive and relevant set of measures in examining national cybersecurity strategies. The research data was subsequently collected by reviewing and analysing the most recently published national cybersecurity strategies of nations chosen for review. The data was collected and collated into the existing research data frameworks for analysis with the current data sets giving a new set of data to assist in answering our research question.

The literature review informed the research of the advances in cybersecurity and developments in the field. The literature review objective for the research was to form a holistic understanding of the topic, cybersecurity and related topics. The literature review was conducted by investigating trends in cybersecurity and searching a combination of information sources both academic and governmental, international websites. The obtainment of national cybersecurity strategies per country for review was collated and sourced from the governmental websites of the countries. Other sources of global and international importance were identified such as the European Union, NATO to understand international laws, policy documents and communications pertaining to cybersecurity.

1.4 Chapter Synopsis

Chapter one provides a background to the study with an introduction and brief background to cybersecurity. The chapter outlines the research aims and research methodology used. Chapter two, The literature review is broken into two sub categories, “Cybersecurity: A Consequence to Connectivity” and “The Internet: The Need to Regulate”. The foremost explores the rise of the cyber domain focusing on cybersecurity risks with examples of high

profile attacks. The latter provides a high-level outline of responses to cybersecurity by the two-major international economic, political and military organizations; the European Union and NATO. The chapter also looks at the measures undertaken by Ireland in response to global and European measures. Chapter three: Framework Analysis examines published national cyber security strategies and compares other nations strategies to Ireland's strategy. The purpose is to measure Ireland's preparedness for cyber security by comparing to other countries and consequently, where applicable, provide recommendations to strengthen Ireland's strategic direction and assist in the development of a new national cyber security strategy. Chapter four; Discussions and Conclusions appraises the key findings of the research summarizing the conclusions of chapter three's framework analyses, a review and analysis of National cyber security strategies developed by nations.

Chapter Two: Literature Review

2.1 Cybersecurity: A Consequence to Connectivity

2.1.1 Introduction

This chapter will elucidate the cybersecurity realm, exploring the rise of the cyber domain to recent developments in cybercrimes and the current landscape. This portion of the study will provide a background to cybersecurity by firstly reviewing literature definitions of cybersecurity terminology, examining the threat actors involved in cybercrimes and attacks. The chapter will focus on the increase in high profile sophisticated attacks providing examples of such attacks to demonstrate the considerable risks of a cyberattack in an effort to highlight the importance of cybersecurity.

2.1.2 Defining Cyber Security

The literature reviewed revealed the shift in defining cybersecurity from a predominately technological focus to a broader all-encompassing perspective surpassing technical to include aspects such as management, law and policy making to strategize and plan for the protection of cyberspace. The lack of a precise definition to the new wealth of information presented is causing challenges for leaders and policymakers. Cyberspace historically belonged to the IT department as a technology based issue. This is no longer the case as the reliance and usage of IT is now firmly a strategic agenda item within organisations to both strategize and protect. Cyberspace now demands further intervention from non-technical backgrounds to ensure a safe environment for all society. The lack of unified terminology and definitions further exacerbates the issue to govern cyberspace and set laws in combating illicit activities that are ever increasing in this new age of cyberspace. Cybersecurity is no exception. Cyberspace, cybercrime and cybersecurity are continuously used interchangeably with many variations. From a technical perspective, the most common definition of cybersecurity is defined by (TechTarget, 2018), "Cybersecurity is the protection of Internet-connected systems, including hardware, software and data, from cyber-attacks. In a computing context, security comprises cybersecurity and physical security both are used by enterprises to protect against unauthorized access to data centres and other computerised systems. Information security, which is designed to maintain the confidentiality, integrity and availability of data, is a subset of cybersecurity." (TechTarget, 2018).

(Craigen, et al., 2014), agree that cybersecurity is a broadly used term with highly variable definitions mainly focusing on the technical view. (Craigen, et al., 2014), posit that a definition of cybersecurity should be reached that is, multi-dimensional to meet the challenges presented by cybersecurity across all disciplines to allow all to collaborate in combatting cybersecurity challenges. (Craigen, et al., 2014), define cybersecurity as "The organisation and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights". (TechTarget, 2018).

(Swire, 2018), agrees with the interdisciplinary dimensions of cybersecurity proposing a pedagogic Cybersecurity Framework to focus on the non-technical elements of cybersecurity by introducing three additional elements to the Open Systems Interconnection Model (OSI model) to include; Layer 8,9,10 namely organisations, governments and international. The OSI model is a model developed by ISO to understand the steps in data processing through the different stages of transmission. The model has seven layers that data passes through; physical, data link, network, transport, session, presentation, and application. The objective of (Swire, 2018) recommendation is to provide a 'holistic understanding of the cybersecurity ecosystem" for non-computing professionals or non-technical professionals studying cyber security.

(Luiijf, 2013) posit the lack of a harmonised common definition of cybersecurity and other cyber-related definitions could be a cause of confusion among nations especially when discussing international approaches to cyber threats on a global level. (Luiijf, 2013) refer to the definition provided by Russian-US bilateral working group who drafted an international cyber terminology framework, cybersecurity as "a property of cyber space that is an ability to resist intentional and unintentional threats and respond and recover"

Chapter three; Framework Analysis, review and analysis of national cybersecurity strategies support this theory of different definitions of cybersecurity by providing cybersecurity definitions provided by nations in table 1. The research concludes no unified definition is used among the nations when describing cybersecurity with many variations in scope. The analysis provides a table summary of the diverse definitions of nations.

2.1.3 Who is responsible for Cyber Attacks?

Cybercriminals are criminals who use computers to commit a crime. Cybercriminals can be prosecuted for the crime like any other crime such as theft and fraud. Cybercriminals are often referred to as ‘Hackers' if the access to a computer system was obtained illegally, however, cybercriminals use different forms to extort information for criminal purpose such as social engineering where entry to the computer system is not made by infiltrating the system but by misleading the individual to provide personal details. Hackers and Cybercriminals are often referred to interchangeably, conversely the term Hacker has expanded over the past decade to include different variations of ‘hacker'; White-hat, Grey-hat, Black-hat. The legality and legitimacy of their actions determine the shade with white and grey consider their hacking activities legitimate to infiltrate sites and expose information for political purposes. (Senker, 2017). White-hat hackers are employed by security companies, governments and large organisations to expose their vulnerabilities. White hat hackers are also referred to as ethical hackers. Grey-hat hackers believe they too are working for the greater good by publicizing security vulnerabilities and are prepared to break the law to expose. Black-hat hackers commit fraud by stealing data and seizing control of websites for ill intent. (Senker, 2017). It is now considered ‘easy' to purchase hacking services or stolen data on the darknet. Hacking is now very much a profession where organizations recruit hackers to test, analysis and identify an organizations network weakness's if they exist. Large Organizations commonly hold ‘Hackathons' to test the organization's systems and networks and discover vulnerabilities.

Some hacker’s grey-hat hackers believe their work is ethical as they work on behalf of society exposing wrongs of governments, political parties and large organizations however mostly performing illegal actions in obtaining and exposing information. There are many groups operational like this and some have exposed and provided great insights into an otherwise undercover world of white-collar crime.

The Mossak Fonseca leak exposed the financial exploits of some of the wealthiest individuals on the planet from celebrities to drug traffickers and fraudsters who had set up tax havens to keep financial transactions hidden. The disclosure of 11.5 million records from the law company based in Panama exposed internal records of how law companies and banks sell financial secrecy to the wealthy. These services are used to hide corrupt practices and tax invasion. Whistle-blowers disclosed the documents. The papers and documents were released through the Darknet using hacking techniques. In terms of the law, these whistle-blowers unlawfully exposed secret documents and have committed a cybercrime? Alternatively, are they activists

exposing the corruption of influential people? This is the conundrum of grey hat activist hackers. (Senker, 2017).

Edward Snowden, collected and released top-secret US National Security Agency documents regarding the surveillance practices of the United States, "I'm willing to sacrifice [my former life] because I can't in good conscience allow the US government to destroy privacy, internet freedom and basic liberties for people around the world with the massive surveillance machine they're secretly building" (Biography, 2018).

An increase in high profile cyber-attacks have been carried out globally with speculation of responsibilities by nation states or state sponsored. The following sections further examines high profile, highly disruptive cyber-attacks on countries and critical infrastructures where it is speculated to have country involvements.

The Council on Foreign relations have developed an online tracker namely; The Cyber Operations Tracker," The Digital and Cyberspace Policy program's cyber operations tracker is a database of the publicly known state-sponsored incidents that have occurred since 2005" (The Council on Foreign Relations, 2019). The Cyber Operations tracker contains almost 200 state-sponsored attacks by 18 countries since 2005, including 20 in 2016. (World Economic Forum, 2018)

2.1.4 Cyber Attacks on Critical Infrastructures

"Whilst destructive attacks around the world remain rare, they are rising in number and in impact." (GOV.UK, 2016). In response to this, nations are developing offensive cyber capabilities, including destructive ones. Nations are speaking openly of protection methods in responding to the increased cyber threats posed by other nations. Both the UK and USA discuss cyber threats by other nations in their national cyber security strategies and how they plan to address these issues. Several cyberattack incidents are provided in the following sections that demonstrate the severity of cyber-attacks and cyber warfare.

Ukrainian Power Outage

Described as the first of its kind cyber-attack; an attack on a country's essential services, Ukraine's National power company Ukrenergo experienced a power blackout in the countries capital Kiev. The utility company believes the attack was the result of a cyber-attack, a series of breaches to bring down its services. The attack cut the lights to 225,000 homes and

interfered with the efforts to restore services to the capital. "The attack was the first example of hackers shutting off critical energy systems supplying heat and light to millions of homes" (Reuters, 2017).

"When the lights went out in northern Kiev on Dec. 17-18, power supplier Ukrenergo suspected a cyber-attack and hired investigators to help determine the cause of a series of breaches across Ukraine" (Reuters, 2017). The investigation continues by both law enforcement officials and cybersecurity experts to the events that led to the outage and to determine the penetration points in the computers infrastructure. Although Ukrenergo recognises it was an intentional attack Ukrenergo has not blamed anyone on the attack; however Ukrainian security officials have blamed the attack on Russia (Reuters, 2017). This view is shared by many global cybersecurity analysts who have a much broader theory about the endgame of Ukraine's hacking epidemic: They believe Russia is using the country as a cyberwar testing ground—a laboratory for perfecting new forms of global online combat. Moreover, the digital explosives that Russia has repeatedly set off in Ukraine are ones it has planted at least once before in the civil infrastructure of the United States. (Greenberg, 2017).

Estonian Outage

Estonia is dubbed E-stonia due to its electronic status with claiming the most advanced e-government in the world and the first country to offer e-residency. Estonia is one of the most wired and innovative countries with a high level of start-ups and educated innovated workforce. Both government and Estonians strive to create the ideal information society. (Keen, 2018).

However, Estonians today are not only known in cyber talk for its digital advances but due to the unfortunate circumstances of a cyber-attack on the county. Today Estonia is also considered to be a cybersecurity hotshot in the aftermath of what is reported to be one of the first countries to fall victim to a cyber-attack by another country. An article on the BBC news website aptly titled introduction as 'From Outrage to Outage' posits the reason and motives behind the cyber-attack in April 2007 that lasted over a period of three weeks. (Damien McGuinness, 2017). The Outrage began when Estonian authorities decided to move a World War Two memorial statue named the Bronze soldier to a less prominent position in the capital of Tallinn. For ethnic Russian speakers in Estonia, the bronze soldier represented the USSR's victory over Nazism however to ethnic Estonians the bronze soldier symbolised half a century of Soviet oppression, believing the Red Army soldier, the bronze soldier were not liberators but occupiers of Estonia. When news broke of the authorities' plans to move the memorial to the

outskirts of the city the news caused outrage and the situation in the capital quickly escalated. The situation was further exasperated by media outlets and the spread of false news claiming the destruction of both the statue and Soviet war graves. Major rioting and looting ensued on the streets of the capital leading to many injured and one death.

On April 27th, 2007, the riots of the previous day were followed by a major cyber-attack to Estonia's online services. The cyber-attack led to the taken down of Estonian's key websites and online services of government bodies such as parliament websites, banks and media outlets to name a few. The outage was caused by unprecedented levels of internet traffic and spam emails sent by botnets to create a mass amount of traffic and large volumes of automated online requests which eventually led to the swamping of servers. The consequences of the attacks for the citizens of Estonia included disruption and non-availability of banking services, cash machines were out of action, government communications affected and the inability of newspapers and broadcasters to deliver the news. What is now commonly referred to as the 'Bronze Soldier Attacks' is considered the first suspected state-backed cyber-attacks on another nation, Russia is again suspected of being involved in the attacks however there is no concrete evidence that the attacks were carried out by the Russian government. What is known is the attacks came from Russian IP addresses, online instructions were in Russian, and Estonia's appeal to Moscow were ignored. (Damien McGuinness, 2017).

Today Estonia is considered an expert country in cyber defence. "It was a great security test. We just don't know who to send the bill to," says Tanel Sepp, a cybersecurity official at Estonia's Ministry of Defence. (Damien McGuinness, 2017). The Estonian attack led to pressures on NATO ministers to respond to cyber-attacks. NATO since released its policy on cyber defence and in 2008 set up its centre of excellence in the capital of Estonia, Tallin, NATO Cooperative Cyber Defence Centre of Excellence (COCDCE).

Stuxnet

Stuxnet holds great significance to the advances and developments of cyber-attacks and cyber warfare. Stuxnet had been described as "one of the most notable weapons in history; and not just cyber history, but history overall" (Singer, 2015).

Stuxnet is the name given to the virus that crippled over 1000 industrial centrifuges in the Iranian Nuclear Plant, Natanz. The attack is highly speculated as a state-sponsored attack due to the sophistication of the virus, the expertise and time to develop. The virus was a targeted attack on the critical infrastructure of the plants Supervisory Control and data acquisition

(SCADA) system and the Programme Logical Controllers (PLC's) operating the centrifuges which were used to separate nuclear materials.

Stuxnet is described as a highly sophisticated targeted, malicious computer virus. The virus was first discovered in 2010 by computer security experts. The Stuxnet virus target was eventually identified as; Natanz, a uranium enrichment infrastructure plant in Iran.

Security experts became alert to a worm of unknown origin that was spreading across the world embedding itself in control systems, such as SCADA systems which are used to monitor and run industrial processes in industrial plants such as power generation facilities and water treatment centre (EBSCO). The bulk of infections centred in Iran where 60% of the worm was detected. At first security experts thought this was a result of poor defences of SCADA systems within Iran and not of a targeted virus. (Singer, 2015).

Experts believe Stuxnet was in development since as early as 2005 before discovery in 2010. Stuxnet bares all the hallmarks of nation-state support due to its sophistication. The two countries believed to be behind the development of Stuxnet is the USA and Israel. The development of Stuxnet has been dubbed as "Operation Olympic Games" a campaign to sabotage by means of cyber disruption, it it is one of the first known uses of offensive cyber weapons. (Redpacket Security , 2016).

Stuxnet had many sophisticated traits, it sought out computers and networks that met specific configuration requirements and did no harm to others that did not meet the criteria. Stuxnet searched for Siemens software and if not found the application made itself redundant. The worm also had safeguards that only allowed the worm to spread to a maximum of three other computers and erased itself on a specific date in order to go undetected. The worm operates in a layered attack on three different systems; Windows operating systems, STEP7 software application and Siemens S7 PLCs. The virus initially spread via Microsoft Windows, and targeted Siemens industrial control systems, systems used in industrial process control. (Steven Cherry, 2011).

"A new kind of weapon long speculated about but never seen, a specially designed cyber weapon, had finally been used. Prior cyber "attacks" had stayed within the digital realm, usually involving the theft, disruption, or manipulation of information. Stuxnet did that, but caused something new, physical consequences." (Singer, 2015).

Ralph Langner, the researcher who identified that Stuxnet infected the PLCs described the effects of Stuxnet "as good as using explosives" against the facility. In fact, it was better. The victim had "no clue of being under a cyber-attack." “The Stuxnet attack has far-reaching cybersecurity and policy implications, as it demonstrates that nation-states are susceptible to crippling cyber actions from other nation-states or private entities”. (Lachow, 2011) The concern highlighted by (Lachow, 2011) posits what are the implications of Stuxnet; is it a case of other countries now developing cyberweapons based on the success of Stuxnet. The Stuxnet virus is increasingly becoming publicly available, and it is likely that at least some countries and/or organizations will attempt to copy the Stuxnet attack.

Syrian Hospital

The Telegraph news article by (Dixon, et al., 2018) titled “Hackers 'led warplanes to Syrian hospital' reports on claims made by British surgeon, Mr. David Nott’s, a renowned consultant, who received an OBE for his work in training surgeons in war torn countries.

Mr. Nott’s suspects his home computer was hacked to obtain coordinates of a secret underground hospital in war-torn Aleppo, Syria. Nott’s, fears his computer was targeted and consequently led the hackers to a hospital being bombed by suspected Russian warplanes. From his London office, Mr Nott’s remotely consulted with surgeons in the M10 hospital via Skype and WhatsApp that was subsequently broadcast by the BBC and available online. Weeks later the hospital was bombed with what is known as a “bunker buster” a sophisticated bomb that can target underground locations. This is one of the reasons Russia is suspected of the attack. The attack was directly aimed at the operating theatre that Mr Nott’s had connected within the weeks previous hence why the timing and exact location leads him to believe the hacking of his computer and phone had disclosed the coordinates of the M10 hospital. “The operation was the only time co-ordinates came out of that operating theatre” (Dixon, et al., 2018). Nott’s theory is further endorsed in the article by Professor Woodward, Surrey Centre for Cyber Security who confirms the hacking of Mr. Nott’s computer later after the broadcast as “It is a method that has been used by governments and law enforcement agencies for several years, he said, adding: "It is a fairly classic way of getting information. You don't need to do it at the time; you can break in at your leisure." (Dixon, et al., 2018). Mr. Nott’s and the International Committee of the Red Cross are advocates now of warning of the dangers of hacking as a war crime.

2.1.5 Cybersecurity protection methods

Cybersecurity protection can be implemented by organisations to prevent attacks to both computers and networks safeguarding data and essential services. Cybersecurity includes using firewalls, intrusion detection and detection prevention systems, software to detect virus's anti-software, encryption and login verification systems. Organisations, in order to protect their computer and network systems have an obligation to ensure the correct protection measures are in place to prevent security breaches and attacks where possible. The internet has had little regulation and ran mainly by private organisations. Governments are now becoming enforcers of security measures for the protection of nations and citizens as the number and sophistication of cyber-attacks continues to rise. The regulatory frameworks by nations is aiming to provide greater control, transparency, awareness and compliance to standards on cybersecurity. Cybersecurity requires joint efforts from both the public, private sector to adhere to the standards, guidelines and legislation set out by governments. Individuals also play a part in the use of cyberspace and to act inappropriate and safe manners taken precautionary measures as one would in society.

Doomsday of a cyber-attack could bring down our financial services, cripple our nation’s infrastructure, cut national grid power to homes, derail trains, interfere with our air space, oil refineries and gas pipelines could be used as weapons of mass destruction.

The concern and prediction of cybersecurity experts is the reality of the capabilities of cybercriminals or hackers whether considered ethical or acting on behalf or funded by countries is the ability to penetrate networks to cause mass destruction is real.

2.1.6 Conclusion

Cyber-attacks have grown in sophistication in recent years as the technical abilities of cybercriminals have advanced cybercrimes. Previously associated risks of cybercrimes to both individuals and organisations were typically associated with exposure of personal data and information resulting in financial losses. Today personal data and organisational data is holding both individuals and organisations to ransom but the level is increasing to mass destruction of critical infrastructures. The new threat actors hold different motives than financial gain and present new threats to nations. The threat of attacks to nations targeting national assets and infrastructure is resulting in the protection of ICT now firmly a national and global concern. Cybercrimes have extended from identity theft to attacks on countries in acts of sabotage, espionage, ransom and war crimes or otherwise referred to Cyberwarfare. Nations and world

leaders are now cognisant of the risks involved with cybercrime and need to ensure protection and safety of citizens, national infrastructure and services. The correct governance and legislation must be introduced to provide this but also must protect the benefits of cyberspace and the internet that society has now become accustomed. The European Commission's Cyber Security Strategy considers governments as having a significant role in ensuring a free and safe cyberspace. The strategy states; by safeguarding access and openness, and to respecting and protecting fundamental rights while online to maintain the reliability and interoperability of the internet (European Union, 2018).

The response taken by governments and nations is to develop strategies and implement laws to manage and deal with the threats presented by cybercrimes however this is a challenge as the speed at which technology is changing is making this task more difficult along with the fact that a significant portion of the internet is owned and operated by private sectors. Governments must also be mindful of the many benefits the internet has brought to society such as connecting people, promoting political and social inclusion worldwide, breaking down barriers, freedom of expression. (Commission, 2013). This openness that is created by the internet is adding to the complexities for ensuring the correct regulations are in place in order to control and combat cybercrimes and not people’s freedom in cyberspace.

The accountability for securing cyberspace is a collaborative effort. Greater governance and laws of recent times are put in place by international institutes from a strategic level. The EU and NATO are now taken an active role in cyber security measures however cyber security is still a national level responsibility. The EU is providing greater governance of organizations to ensure the protection of personal data and protecting of networks against harm where NATO focuses on security and defence aspects.

The following chapter discusses the response to cybersecurity at international level.

2.2 The Internet: The need to regulate

2.2.1 Introduction

This chapter will outline the responses to cybersecurity by the two-major international economic, political and military organizations; the European Union and NATO. This chapter will also look at the measures undertaken by Ireland in response to global and European measures.

"Currently, cyber security as such is not independently regulated internationally; therefore, the role of the EU and NATO in ensuring cybersecurity has become particularly significant." (Štitilis, 2017)

2.2.2 Response to Cybersecurity

The world-wide web and internet to date has mainly been operated by private enterprises with little or no governance since its inception. As we globally continue to move towards digital economies for national wealth and prosperity with initiatives like the EU digital agenda the necessity to secure the internet has increased. The new threat landscape has also increased awareness among nations and the need for greater governance of cyberspace.

The EU digital agenda launched in May 2010, was introduced to enable Europe to get the benefit out of digital technologies after the downturn in 2008. "The overall aim of the Digital Agenda is to deliver sustainable economic and social benefits from a digital single market based on fast and ultra-fast internet and interoperable applications" (European Commission, 2010). Subsequently, the digital agenda was the catalyst for the EU's development of its first cyber security strategy.

For NATO, the cyber-attack on Estonia was the springboard to cyber discussions of its members. The challenges now for international organisations and nations is to find the balance between protecting society and individuals in cyberspace whilst maintaining the open and free fundamentals the internet holds. The Cybersecurity Strategy of the European Union extant the benefit to society of cyberspace as the open and free cyberspace has promoted political and social inclusion worldwide, however the European Union also acknowledges "For cyberspace to remain open and free, the same norms, principles and values that the EU upholds offline, should also apply online. Fundamental rights, democracy and the rule of law need to be protected in cyberspace." (European Union, 2018). Whereas NATO has affirmed that

international law applies in cyberspace also recognizing cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land and at sea (North Atlantic Treaty Organisation , 2018). Both the EU and NATO are strategically assisting member countries in securing cyber space both organisations outline their need to protect their own assets to cyber threats and the responsibility nationally to cybersecurity.

2.2.3 European Union Response to Cyber Security

(European Union, 2018), jointly issued the cybersecurity strategy of the EU in 2013 by the European Commission and the High Representative for Foreign Affairs and Security Policy on the EU cyber security strategy formerly titled "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. The strategy proposal was published in two parts; The EU cyber security strategy and the European Commission's proposal for a directive on network and information security. The proposal document to the EU parliament proposes that the same norm, principles and values that the EU upholds offline, should also apply online. Fundamental rights, democracy and the rule of law need to be protected in cyberspace for cyberspace to remain open and free (Commission, 2013). The European Union emphasizes in its official communications the recognition that the EU's cybersecurity is equally important as security in the physical space. (Kovacs, 2018).

The EU response to cyber security is derived from digital initiatives such as the European digital agenda initiated to strengthen the European digital market in the aftermath of the 2008 downturn since then the EU have continued with initiatives to strengthen the EU's cyber security.

European Union Cyber Security Strategy

The European Union Cyber Security Strategy "outlines the EU's vision and the actions required, based on strongly protecting and promoting citizens' rights, to make the EU's online environment the safest in the world". (Commission, 2013). The strategy is based on five principles that will be priorities for the future of the European Union. The Strategy presents its five principles (priorities) as the following: Achieving cyber resilience, drastically reducing cybercrime, developing cyber defence policy and capabilities related to the Common Security and Defence Policy (CSDP), Develop the industrial and technological resources for cybersecurity, establish a coherent international cyberspace policy for the European Union and promote core EU values". (Commission, 2013).

Network Information Systems Directive

The European Commission further proposes in its strategy document a directive on network and information security. This is referred to as the NIS Directive. The main objective of the directive is to ensure that there is a common high level of cyber security across member states. The Network and Information Security (NIS) Directive proposed in March 2014 formed part of the European Union's cybersecurity strategy. "The NIS Directive is the first piece of EU-wide legislation on cybersecurity. It provides legal measures to boost the overall level of cybersecurity in the EU." (European Commission , 2018). The objective is to protect critical national infrastructure. The European Union formally adopted the directive with transposition deadline on the 09th May 2018. The NIS requires EU member states to identify Operators of Essential Services (OES) such as energy, transport and banking services and ISP providers to follow the framework outlined in the directive to secure these infrastructures. "The directive is intended to foster co-operation between EU nations while legislating expected security requirements for all essential services." (Allison, 2017). The directive provides legal measures to boost the overall level of cybersecurity in the EU. The directive stipulates member states must be prepared and adequately equipped by implementing the following at national level; Computer Security Incident Response Team (CSIRT), A competent national NIS authority, CSIRT Network, and cooperation among all the Member States. (European Commission , 2018).

European Union Agency for Network and Information Security (ENISA) Agency

ENISA is a centre of network and information security expertise of the EU for its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. (ENISA, 2018). "ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU". (ENISA, 2018).

Cyber Security Package

The Cyber Security Package is a product of the EU proposing new initiatives for cyber security. Following a midterm review of the digital single market in May 2017, the commission identified cyber security as a key area for further works. The Commission adopted a cybersecurity package on the 13th September 2017 outlining a number of improvements and initiatives. The

cyber security package builds on existing instruments. "Among the measures to increase the EU resilience to cyber-attacks, a legislative proposal to strengthen ENISA has been already published in September 2017 cybersecurity act, which gives it a permanent mandate and sets up a voluntary EU certification framework for ICT products and services". (European Parliment, 2019) . Among other measures is the updating of the EU's cyber security strategy.

Cyber Security Act

The European Commission proposed the Cybersecurity Act in September 2017 as part of the above mentioned cyber security package which set out a wide-range of measures to strengthen cyber security in the EU. The Cybersecurity Act was adopted by the Members of the European Parliament on the 12th March 2019. "The new EU Regulation gives ENISA, the European Union Agency for Cybersecurity, a permanent mandate and strengthens its role. The Act also establishes an EU framework for cybersecurity certification, boosting the cybersecurity of digital products and services in Europe".

The Cybersecurity Act:

- strengthens the ENISA by granting to the agency a permanent mandate, reinforcing its financial and human resources and overall enhancing its role in supporting EU to achieve a common and high-level cybersecurity. (European Commission , 2019)
- establishes the first EU-wide cybersecurity certification framework to ensure a common cybersecurity certification approach in the European internal market and ultimately improve cybersecurity in a broad range of digital products (e.g. Internet of Things) and services. (European Commission , 2019)

Budapest Convention

The Convention on Cybercrime of the Council of Europe (CETS No.185), known as the Budapest Convention, is the only binding international instrument on this issue. It serves as a guideline for any country developing comprehensive national legislation against Cybercrime and as a framework for international cooperation between State Parties to this treaty. "The Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception. Its main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society

against cybercrime, especially by adopting appropriate legislation and fostering international co-operation" (Council Of Europe, 2018)

European Union General Data Protection Regulation

The General Data Protection Regulation replaced the existing data protection framework under the EU Data Protection Directive. "The GDPR emphasises transparency, security and accountability by data controllers, while at the same time standardising and strengthening the right of European citizens to data privacy. " (Data Protection Commission, 2018)

The new EU General Data Protection Regulation will give people in the European Union more protection against misuse of their personal data. The new legislation came into force on the 25th of May 2018. The law means greater protection of personal data for all citizens in all EU countries and applies to companies processing EU citizens' data, whether they are based in the EU. Non-compliance of the GDPR can result in heavy penalties to organisations and reputational damage. The law also implements a stricter regime around the reporting of data breaches. Companies must report any data breaches to the Supervisory Authority (SA) within 72 hours of becoming aware of them.

The main changes implemented in the general data protection include; Increased Territorial Scope (extra-territorial applicability), Penalties, Consent, Breach notification, right to access, right to be forgotten, Data portability, privacy by design & Data protection officers. (EU GDPR, 2018). Similarly, to the EU data protection Acts, American states have enforced 'The notice of security breach act' to which organizations must notify of any data breaches.

2.2.4 Europol Cyber Security

Interpol, the world's largest policing organisation and Europol the European cross border policing network both released reports on the threats of cybercrimes as one of the top priorities to combat for the coming years as it colludes organised crime groups are targeting online organisations for a multitude of criminal reasons. (Europol, 2018). The response by world leaders to cybersecurity globally, nationally and at the EU level is in-line with reporting of both organisations. (Allison, 2017), the article focuses on the policy framework set out by the European Police Commission (Europol). The article discussed several topics including "umbrella organization for all of the law enforcement agencies in the European Union, several crimes identified by the Serious and organized crime threat assessment (Socta) framework

including cybercrimes, drug production, trafficking and distribution and smuggling, and increase in number of financial transactions taking place electronically."

2.2.5 NATO Cyber Defence

NATO terminology refers to cybersecurity as cyber defence. "NATO's purpose is to guarantee the freedom and security of its members through political and military means". (North Atlantic Treaty Organisation , 2018). The organisation approved its first policy on cyber defence in January 2008 in the aftermath of the Estonian cyberattacks and following requests from allied defence ministers. "NATO's focus in cyber defence is to protect its own networks (including operations and missions) and enhance resilience across the Alliance." (North Atlantic Treaty Organisation , 2018). "NATO has affirmed that international law applies in cyberspace. In July 2016, Allies reaffirmed NATO's defensive mandate and recognized cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land and at sea. At the same time allies pledged to enhance their cyber defences. NATO allies acted on the pledge with enhancing its cyber defences and continue to develop and implement cyber security measures such as the "NATO Cyber Rapid Reaction teams are on standby to assist Allies, 24 hours a day, if requested and approved". (North Atlantic Treaty Organisation , 2018)

In 2018, Allies agreed to set up a new Cyberspace Operations Centre as part of NATO's strengthened Command Structure. They also agreed that NATO can draw on national cyber capabilities for its missions and operations. (North Atlantic Treaty Organisation , 2018)

"NATO and the European Union (EU) are cooperating through a Technical Arrangement on cyber defence that was signed in February 2016. Considering common challenges, NATO and the EU are strengthening their cooperation on cyber defence, notably in the areas of information exchange, training, research and exercises". (North Atlantic Treaty Organisation , 2018).

2.2.6 United Nations

ITU is the United Nations specialized agency for information and communication technologies. "ITU is founded on the principle of international cooperation between governments (Member States) and the private sector (Sector Members, Associates and Academia)."
(ITU , 2019). "The work of the Groups of Governmental Experts has focused on the following topics: Existing and emerging threats, how international law applies in the use of ICTs, Norms,

rules and principles of responsible behavior of States, Confidence-building measures, Capacity building” (United Nations Office of Disarment Affairs , 2018).

António Guterres, the United Nations Secretary-General has expressed concern over the malicious use of ICTs. “He has therefore made the promotion of a peaceful ICT-environment one of his key priorities” (United Nations Office of Disarment Affairs , 2018). “Guterres has called for global action to minimize the risk posed by electronic warfare to civilians. Guterres lamented that “there is no regulatory scheme for that type of warfare,” noting that “it is not clear how the Geneva Convention or international humanitarian law applies to it” (World Economic Forum, 2018).

The EU strongly promotes the position that international law, and in particular the United Nations (UN) Charter, applies in cyberspace. As a complement to binding international law, the EU endorses the voluntary non-binding norms, rules and principles of responsible State behavior that have been articulated by the UN Group of Governmental Experts. It also encourages the development and implementation of regional confidence building measures, both in the Organization for Security and Co-operation in Europe and other regions. On a bilateral level, cyber dialogues will be further developed and complemented by efforts to facilitate cooperation with third countries to reinforce principles of due diligence and state responsibility in cyberspace.

2.2.7 Ireland Cybersecurity

Irelands National Risk Assessment has noted cybersecurity as a discrete strategic risk since its conception in 2014. Irelands National Risk Assessment, 2017, chapter 5 is dedicated to technological risks. The 2017 assessment stated, "the fact that Ireland is home to a large number of international data Centre's means that a serious attack or cybersecurity failure could have a damaging impact not just on our reputation, but also on our economy". (Department of the Taoiseach, 2018). Ireland published its first National Cyber Security Strategy in September 2015. The strategy is a high-level outline of security efforts. The document states its objectives as, "set out the Government's approach to facilitating the resilient, safe and secure operation of computer networks and associated infrastructure used by Irish citizens and businesses." Furthermore, affirming the document "sets out the high-level strategic goals that form the basis of national policy in this area and establishes the measures taken in respect of each" (Department of Communications, Climate Action & Environment, 2015-2017).

Minister White said: "This Strategy published today sets out how Ireland addresses cyber threats and protects against them. Ireland's digital economy contributes 5% of national GDP and provides employment for over 100,000 people. That's why protecting personal data, sustaining investment and ensuring the continued reliable functioning of information and communication technologies, and of the Internet, are priorities for Ireland."

The Irish Department of Communications Energy and Natural Resources (DCENR) released The National Cyber Security Strategy (2015-2017) on the 20th July 2015 based on the European Union Cybersecurity strategy. The document states the government objectives and sets out the approach to "facilitating the resilient, safe and secure operation of computer networks and associated infrastructure used by Irish citizens and businesses" (Department of Communications Climate Action and Environment, 2018). The high-level strategic goals outlined in the document form the basis of the national policy.

Ireland National Cybersecurity Centre

The establishment of the European Network and Information Security Agency (ENISA) and subsequent national CSIRT support teams are both efforts by the EU to strengthen collaboration of cyber security expertise across the EU. CSIRT teams are also a mandatory requirement as per the NIS Directive. Further to this Ireland in 2014 established the National Cyber Security Centre within the DCENR and the development of the Computer Security Incident Response Team (CSIRT-IE). The CSIRT team assists public sector organisations in their response to computer security incidents and providing advice to reduce threat exposure." (Department of Communications Climate Action and Environment , 2018)

2.2.8 Conclusions

As the lines of physical society and the cyber world continue to blur while we continue our quest of digitalisation and e-economies the challenge is how can we transfer the laws and legislation we have in physical societies to that of the cyber world in order to protect against crime and uphold our civil rights in conjunction. The idealism of the free and open space of cyberspace could be challenged as nations and governments strategize in how best to protect both citizens and economies.

Cybersecurity tools such as; firewalls, intrusion detection and detection prevention systems, software to detect virus's anti-software, encryption and login verification systems are implemented by organisations to prevent attacks to both computers and networks safeguarding

data and essential services. Organisations must protect their computer and network systems however governments are now becoming enforcers of these steps and processes to protect citizens, and human rights as the increased reliance on ICT and the sophistication of attacks and damage caused by such an attack requires for greater governance in cyberspace.

(Kovacs, 2018), states, if these services do not work society, does not work. The importance of cyberspace is no longer questioned, with this comes greater requirements to protect. Accordingly, (Kovacs, 2018), suggests the challenges and threats to cyberspace we are experiencing must be addressed at a strategic level. (Kovacs, 2018). Kovacs further explains the actions of both the European Union and NATO in strategically preparing and implementing regulation to protect cyberspace and critical infrastructures. The aim of both organizations is to ultimately introduce legislation to protect citizens and society. "The missions of the two organisations are complementary, with NATO focusing on security and defence aspects of cyber security, and the EU dealing with a broader, mainly non-military range of cyber issues (Internet freedom and governance, online rights and data protection), and internal security aspects" (Pernik, 2014).

The legislation aims to provide greater control, transparency, awareness and compliance to standards on cybersecurity. Cybersecurity requires joint efforts from both the private sector to adhere to the standards, guidelines and legislation set out by governments. Individuals also play a part in the use of cyberspace and to act in an appropriate and safe manners taken precautionary measures as one would in society.

Understandably challenging it would appear the complexities of cyberspace with private companies owning and operating this space and the fundamental rights of users who have dominated this space where it is rightly reflected by policy documentation in what should be an open and safe place. The problem is like society rules must apply and governance must be enforced to ensure law and order. Cyberspace and the internet is now a world of unknowns a lawless society run by individuals and corporate organizations. The continuation to digitalize both our lives and critical infrastructure and essential resources on the one platform poses too many risks and requires intervention and stronger governance by governments to ensure adequate protection. The EU proposing the NIS, National Infrastructure Strategy to OES: Operators of Essential Services and other recommendations of support to ensure the security of our essential services is the first step in government empowerment to controlling the internet. The explosion of cyberspace poses too many risks and essential services for us not to regulate and implement the law.

The following chapter will review how the above translates to national level by the introduction of national cyber security strategies. The chapter’s main objective is to review and analysis efforts by nations and the implementation of its strategy document

Chapter Three: Framework Analysis

3.0 Methodology

A national cyber security strategy is considered the main document of nation states to meet current and emerging cyber security threats. "It is a plan of actions designed to improve the security and resilience of national infrastructures and services. It is a high-level top-down approach to cyber security that establishes a range of national objectives and priorities that should be achieved in a specific timeframe" (ENISA, 2019). (Luiijf E. B., Nineteen national cyber security strategies, 2013), define a national cyber security strategy as "A national plan of action based upon a national vision to achieve a set of objectives that contribute to the security of the cyberspace domain". The purpose of a strategy document is to "set strategic principles, guidelines, and objectives and in some cases specific measures in order to mitigate risk associated with cyber security". (ENISA, 2019). Furthermore, the requirement for a National Cyber Security Strategy (NCSS) is required by law in EU countries since the transposition of the Network and Information Security directive in 2018. Article 7 of the directive stipulates "each member state shall adopt a national strategy on the security of network and information systems defining the strategic objectives and appropriate policy and regulatory measures with a view to achieving and maintaining a high level of security of network and information systems" (Official Journal of the European Union).

The objective of chapter three is to review and analyse published national cyber security strategies and thus compare other nations strategies to Ireland's strategy. The review will analyse the content and data gathered of a pre-defined selection of national cyber security strategies published. The review will be performed on a set of criteria and a selection of countries strategically chosen for this review. The purpose is to measure Ireland's preparedness for cyber security by comparing to other countries and consequently, where applicable, provide recommendations to strengthen Ireland's strategic direction and assist in the development of a new national cyber security strategy. The review will be conducted by using framework analysis employing two existing frameworks. Appraising two frameworks already available and previously used to compare and analysis published national strategies. The first framework criteria compare the twenty-eight EU member states and EFTA countries (ENISA , 2019). A second framework criteria analysis a selection of global and EU national

strategies (Luiijf E. B., Nineteen national cyber security strategies, 2013). The two chosen frameworks are further described in the below sections.

3.1 Evaluation Criteria

Two evaluation frameworks were chosen for analysis and review to assist in answering our overall research question. This will be achieved by comparing Ireland's strategy to other countries' strategies. The first evaluation criteria are derived from the European Union Agency for Network and Information Security (ENISA). The agency published an updated version of the National Cyber Security Strategy Good Practice Guide in 2016. (ENISA, 2019) The guide provides guidelines to EU countries for developing, designing and implementing a National Cyber Security Strategy. The document sets out fifteen objectives a NCSS should include to have a robust strategy. The ENISA agency conducted an analysis and review of the twenty-eight EU countries against the set of objectives outlined in the ENISA user guide. The review determined if each national NCSS cover each of the objectives within their respective cyber security strategies. The aim of ENISA is to support EU and EFTA countries with developing and updating their respective NCSS documents.

The second analysis framework is obtained from the highly reputable conference journal titled 'nineteen national cyber security strategies' published in 2013 (Luiijf E. B., Nineteen national cyber security strategies, 2013). The research is frequently referenced in academic research papers about national cyber security strategies. The 2013 journal article is an update to the 2010 version of the document where ten national cyber security strategies were used namely, 'Ten national cyber security strategies' (Luiijf H. B., 2011). The 2013 paper reviews nineteen national cyber security strategies globally of eighteen countries. The research reviews two versions of the UK's strategies; 2009 and 2011. The decision to review two UK strategies was based on the closeness of published strategy dates and to political changes that effected the content between the strategies (Luiijf E. B., Nineteen national cyber security strategies, 2013). Subsequently the UK has released a further revision of their NCSS document in 2016. The remainder countries reviewed by (Luiijf E. B., Nineteen national cyber security strategies, 2013) are; Australia, USA, Canada, Czech Republic, Estonia, France, Germany, India, Lithuania, Luxemburg, Romania, Netherlands, South Africa, Uganda, Spain, New Zealand and Japan. Ireland was not part of the review in either of the 2010 or 2013 reviews completed. The analysis criteria used in the journals is replicated for this research to allow us to compare Ireland to the set of criteria outlined in the journal with a selection predetermined countries. The selection process for the countries chosen for review is explained in section 4.5; 'Country selection

process'. The conclusion of the review and analysis intends to identify, if any, Ireland's shortfalls and provide recommendations to strengthen Irelands national cyber security based on findings and best examples of other nations.

3.2 Finding and Analysis

The following sections provides details of the analysis frameworks and subsequent findings per framework analysis chosen.

3.2.1 Review 1 - ENISA NCSS Analysis

The ENISA agencies National Cyber Security Strategy Good Practice Guide 2016, objective is to assist EU nations in the designing and implementing of member states National Cyber Security Strategies (ENISA, 2019). The guide focuses on two stages for building a NCSS; Design and Development of a NCSS and secondly implementing a NCSS. For the implementation stage the guide sets out fifteen objectives that should be included at national level for a robust NCSS. The agency subsequently reviewed each of the EU countries published NCSS documents, comparing to the fifteen objectives, resulting in how many of the objectives are met in their respective strategy documents. The results are made available on the ENISA website via an interactive map. The interactive map provides information per country of each European nations NCSS including objectives achieved in each NCSS. The interactive map can be found here (ENISA , 2019) For this analysis the information from the website is collated per country into a table to display all EU countries and the objectives met per country. The purpose of collating the information is to clearly identify Ireland's NCSS in comparison to the other EU countries against the ENISA criteria, fifteen objectives. Ireland is No. 1 highlighted below with red border.

		1	2	3	4	5	6	7	8	9	10	11	12	13	14
		Ireland	UK	Germany	France	Italy	Poland	Sweden	Spain	Romania	Estonia	NL	Denmark	Finland	Croatia
	Published Year	20/07/2015	29/11/2016	07/11/2016	10/10/2015	02/12/2013	30/11/2017	22/06/2017	03/01/2013	23/05/2013	01/09/2014	21/04/2018	01/05/2018	24/01/2013	07/10/2015
	Objectives achieved	5	12	9	13	15	13	9	15	11	13	7	11	14	7
	Objectives														
1	Develop national cyber contingency plans	Y		Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	
2	Protect critical information infrastructure		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	
3	Organise cyber security exercises	Y	Y		Y	Y	Y	Y	Y		Y		Y	Y	
4	Establish baseline security measures		Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y
5	Establish incident reporting mechanisms	Y	Y		Y	Y	Y		Y	Y	Y		Y	Y	Y
6	Raise user awareness		Y	Y	Y	Y	Y		Y	Y	Y		Y	Y	
7	Strengthen training and educational programmes		Y		Y	Y	Y		Y	Y	Y	Y	Y	Y	
8	Establish an incident response capability	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y
9	Address cyber crime		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
10	Engage in international cooperation	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
11	Establish a public-private partnership		Y			Y	Y	Y	Y	Y		Y		Y	
12	Balance security with privacy				Y	Y		Y	Y		Y			Y	Y
13	Institutionalise cooperation between public agencies		Y	Y	Y	Y	Y	Y	Y		Y				
14	Foster R&D		Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y
15	Provide incentives for the private sector to invest in security measures					Y			Y					Y	

The review table illustrates, of the fifteen objectives outlined in the good user guide Ireland met five of the objectives in its 2015 published NCSS document. In comparison to other nations' NCSS documents Ireland include the lowest number of recommended objectives in its strategy document. According to the ENISA agency review of the fifteen objectives outlined, Ireland mention the following objectives in its 2015 NCSS;

1. Develop national cyber contingency plans
3. Organize cyber security exercises
5. Establish incident reporting mechanisms
8. Establish an incident response capability
10. Engage in international cooperation

The five items achieve the initial requirements set out by the EU strategy document and ENISA NCSS development and NIS directive indicating Ireland has built the minimum into the development of its NCSS document without moving to implantation phase with the remainder of objectives.

The above analysis is derived from findings of the ENISA agency and is provided on their website (ENISA , 2019). however, this research will further analyse and review if Ireland has advanced in any of the objectives by further research to give us a comprehensive analysis of Ireland's status.

3.2.2 Review 2 - Nineteen National Cyber Security Strategies

(Luiijf E. B., Nineteen national cyber security strategies, 2013), analyses nineteen cyber security strategies of eighteen countries to compare and distinguish elements of their NCSSs. The objective of the analyses by (Luiijf E. B., Nineteen national cyber security strategies, 2013) is to review whether the approach of countries is similar considering cyber security is subjected to the same set of threats for all countries globally. The transnational issues of cyber security would suggest a common approach globally to be an objective however the 2013 analysis does not support this and highlights both synergies and weaknesses according to (Luiijf E. B., Nineteen national cyber security strategies, 2013). The research by (Luiijf E. B., Nineteen national cyber security strategies, 2013) looks at common themes expected to be addressed in a NCSS such as the countries strategic objectives, visions and guiding principles. The

research collates each countries data and reviews these themes of the eighteen countries chosen for review.

This research study will follow the same analysis framework used in the nineteen national cyber security strategies. This review will use a selection of pre-determined chosen countries and the latest published strategies per country. The selection of countries is explained in section 4.6 below.

For this study, the analysis framework is used to extend to Ireland for comparison of Irelands efforts defined in its NCSS document published in 2015 where appropriate and compare to other national strategies in the review. The findings can assist in guiding Ireland to develop a robust NCSS. The paper compares definitions of cyber security among nations, general information on the strategies per country, relationships with other strategies, envisioned threats and threat actors. The analysis framework within the document is broken down into the following seven tables listed;

Table 1	Defining Cybersecurity 'National Understanding of cyber security'
Table 2	General Information including; NCSS views on cyberspace and relationship with other national strategies
Table 3	NCSS visions, objectives, guiding principles, identified stakeholders
Table 4	Strategic objectives of the NCSS
Table 5	Guiding principles of the NCSS
Table 6	The NCSS directly addresses types of stakeholder with respect to threats, vulnerabilities and measures
Table 7	Key action lines and planned actions

3.2.3 Selection process for review

The countries selected for review were chosen by combining the two data frameworks general information on national strategies. The reason for combining the two frameworks was to not limit to European countries or (Luiijf E. B., Nineteen national cyber security strategies, 2013) selection criteria to get a varied selection. To facilitate the appropriate selecting of countries for review, data analysis of general information was gathered on the issue date of the strategies under 'general information'. Combining the two frameworks of country data chosen for analysis

between the two studies gives a total of 36 countries. For this research, it is not possible or conducive to review all 36 countries. Of the 36 countries, 33 have updated their national cyber security strategy in the last five years. For the country selection process the approach was to find the most up to date issued NCSS documents of countries. The below table gives the year of the latest published versions of the national NCSS's per country. Considering advancements and changes within the cyber security field the study has chosen to review and analysis the latest published NCSS's, documents published in 2018. The UK has also been chosen for review as Irelands nearest neighbour. A total of eight countries will form the research. The below table illustrates the latest year published of national cyber security strategies per countries mentioned in the above selection process.

Year published	Country
2012	INDIA, BELGIUM, CYPRUS
2013	SPAIN, ROMANIA, UGANDA, ITALY, FINLAND, AUSTRIA, HUNGARY
2014	LATVIA
2015	CZECH REPUBLIC, ESTONIA, FRANCE, JAPAN, S. AFRICA, IRL, PORTUGAL, CROATIA, SLOVAKIA
2016	AUSTRALIA, GERMANY, UK, NEW ZEALAND, BULGARIA, MALTA, SLOVENIA
2017	POLAND, SWEDEN, GREECE
2018	**CANADA, LITHUANIA, LUXEMBURG, NETHERLANDS, USA, DENMARK**

3.3 Defining Cyber security (Table 1)

(Luiijf E. B., Nineteen national cyber security strategies, 2013), posits the importance of providing a definition of cyber security for establishing a common ground when discussing international approaches, further adding the lack of a common, harmonized definition of cyber related terminology may cause confusion between nations. (Shafqat & Masood, 2016), concurs stating disparity lies in the understanding of major key terms namely cyber security, cyber space. "The lack of a common, harmonized cyber-related definition across nations may be a cause of confusion between nations when discussing international approaches to the global cyberspace threats." (Luiijf E. B., Nineteen national cyber security strategies, 2013) P.5.

Table 1 below outlines the definitions of cyber security provided by the eight chosen countries, where available in their published NCSS.

Table 1 - Defining Cyber Security UK, CANADA, USA, NETHERLANDS, DENMARK, LITHUANIA, LUXEMBURG			
1	**IRL**		No definition of cyber security provided
2	**UK**	**Definition**	Cyber security refers to the protection of information systems (hardware, software, and associated infrastructure), the data on them, and the services they provide, from unauthorized access, harm or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures.
3	**CAN**	**Definition**	Cyber security is the protection of digital information and the infrastructure on which it resides on.
4	**USA**		No definition provided
5	**NLD**	**Definition**	Cyber security is the entirety of measures to prevent damage caused by disruption, failure or misuse of ICT and to recover should damage occur
6	**Denmark**	**Definition**	Cyber security encompasses protection against breaches of security resulting from attacks on data or systems via a connection to an external network or system. Cyber security thus focuses on vulnerabilities inherent to the interconnection of systems, including connections to the internet
7	**Lithuania**	**Descriptive**	Cyber security shall mean the totality of legal, information distribution, organizational and technical measures which are aimed at maintaining resistance to factors which pose threat to communications and information systems in cyber space or to the accessibility, authenticity, integrity and confidentiality of digital information transmitted by or processed in such systems, to non-disruptive operation, management of communications and information system or provision of services to these systems, also which serve to restore the usual operation of the communications and information systems.
8	**Luxembourg**	**Definition**	Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies can be used to protect the cyber environment, its organization and its user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment.

Analysis of the selected eight countries NCSS' provided the following information; 2 countries; Ireland's 2015 NCSS and The United States 2018 strategy did not attempt to define cyber security. Both countries discuss cyber security and cyber space at a strategic level without defining the term in the document. The UK define cyber security in a holistic bottom up

approach by describing cyber security as; the protection of information systems and all accompanying information such as software, hardware and infrastructure however interestingly include accidental harm as a cyber security protection. The Netherlands take a similar holistic approach mentioning misuse but not accidental harm. Canada simplistically defines cyber security as protection to both information and system without elaborating on the connectivity or use. Denmark specifically mention 'attacks' of systems via connected networks. Luxemburg and Lithuania descriptively describe cyber security as all encompassing; organizational, legal and technological aspects relating to systems not specifying networked or internet connected, both providing broad descriptive texts to cyber security. The variation of definitions could cause confusion especially when trying to discuss approaches to cyber security at international approaches to the global cyberspace threat. (Luiijf E. B., Nineteen national cyber security strategies, 2013).

Ireland's Department of Communications, Climate Action & Environment, the agency responsible for cyber security in Ireland defines cyber security terminology on its website as "The term 'Cyber Security' refers to the body of technologies, processes, and practices designed to protect networks, devices, programmes, and data from attack, damage, or unauthorized access. As such, it refers to the full range of measures designed to protect IT systems and ensure the confidentiality, integrity, and availability of data services." (Department of Communications, Climate Action & Environment , 2019).
Ireland does not attempt to define cyber security in its strategy document. Ireland should state its definition of cyber security in the next version of cyber strategy to ensure a common understanding to stakeholders of the scope of cyber security.

3.4 General Information (Table 2)

General information is firstly collected of the countries chosen. General information refers to the latest versions/date of issue and size/number of the NCSS document. The following provides a summary of general details of NCSS's collated.

	1	2	3	4	5	6	7	8
General Information	IRELAND, UK, CANADA, USA, NEDERLANDS, LITHUANIA, LUXEMBOURG							
Table 2								
EU or Global (11 EU & 8 Global)	EU	Global	EU	EU	EU	EU	Global	
Country	IRL	CAN	UK	LTU	LUX	NLD	USA	DEN
Previous issue/version		2010	2011					
Latest Issue	07.2015	07.2018	11.2016	08.2018	05.2018	04.2018	09.2018	05.2018
Sizes (pages)	18 pages	35 pages	68 pages	20 pages	23 pages	24 pages	26 pages	56 pages
Relates to;								
National security strategy	☐	■	■	☐	■	■	■	■
Critical infrastructure protection strategy	■	■	■	■	■	■	■	■
National digital agenda	■		■		☐			
EU digital agenda (EC, 2010)	■	n/a					n/a	
National defence strategy	☐		☐	■	■	■	■	■
Addresses cyber threats to:								
Critical infrastructure	■	■	■	■	■	■	■	■
Defence abilities	☐	■	■	■		■	■	■
Economic prosperity	■	■	■	■	■	■	■	■
Globalization		■	■	☐		■	■	■
National security	■	■	■	■	☐	■	■	■
Public confidence in ICT	■	■	■	■	■	■		■
Social life of citizens	■	■	■					
Addresses cyber threats from:								
Activism/extremists		■	■		■		■	■
Criminals/organised crime	■	■	■		■	■	■	■
Espionage	■	■	■	■	■	■	■	
Foreign nations/cyber war		■	■		■	■	■	■
Terrorists		■	■		■		■	
Large-scale attacks	■	■	■	■	■			
Mismatch of technology development and security					■			

Solid colour blue square explicitly mentions term. No fill square implicitly mentions term.

The latest issue date of the strategies are all 2018 and were selected for review based on been the most recently issued NCSS (as per selection process). The strategies give timeframes of issue and vary from two years to five years. Some countries also mention the allocated funding to cyber security during the stated period of the NCSS lifecycle.

The USA states in its latest NCSS version, 2018 that this is its first fully articulated cyber strategy in fifteen years. The 2018 version is the third version of a NCSS published by the USA, the first issue was in 2003 when the term 'cyber security' was relatively unknown. The document does not outline the period before a new revised edition of its strategy will be released or reviewed. The UK NCSS was chosen for review as Ireland's nearest neighbour. The UK's latest NCSS was issued in 2016 and states is for a 5-year period until 2021. The UK government mention funding allocation relating to NCSS period, "UK have pledged 1.5billion to cyber security over the next five years with the objective ' to transform significantly the UK's cyber security" UK NCSS. The Canadian NCSS outlines a five-year strategy and mention in 2018 budget the government vowed 500 million dollars to cyber security over the five-year

period of the NCSS. The Netherlands state the NCSS agenda will be evaluated in 2021 and revised where necessary further stating ninety-five million of structural funding is being reserved for cyber security. Denmark's strategy runs for three years; 2018-2021 dedicating 1.5 billion (DKK) over six years for cyber and information security. Luxembourg and Lithuania strategies for a five-year period with no mentioning of funding.

Ireland's strategy states it is for a two-year period 2015 -2017. The Department of Communications, Climate Action and Environment (DCCAE) website inform a new Irish strategy will be released late 2018 however during this research we are now aware as of the 19th March 2019 a public consultation and call for comment to the next Irish NCSS is currently in place until the 1ST May 2019. For Irelands 2015 strategy a funding of one million was allocated for cyber security. Funding for Irelands cyber security endeavours for the period of 2015-2017 of one million euros was inspected by the Irish government appointed agency, Office of the Comptroller and Audit General. The 2017 examination reviews the progress made since the establishment of the National Cyber Security Centre (Office Of The Comptroller & Auditor General, 2017).

The Irish consultation into the next revision of Irelands NCSS and the findings of the Office of the Comptroller and Audit General report is further discussed in Chapter 5; Findings and Recommendations.

Table 2, General information is further broken into three specific categories pertaining to the strategy; 1. Relates to…., 2. Addresses cyber threats to…., 3. Addresses cyber threats from….

Paragraphs 4.7.1, 4.7.2, and 4.7.3 summarize the key findings as illustrated in table 2.

3.4.1 Relationships with other national strategies

(Luiijf E. B., Nineteen national cyber security strategies, 2013) discusses one of the aims of a NCSS is 'to convey one's national intent to other nations and stakeholders' (Luiijf E. B., Nineteen national cyber security strategies, 2013, p. 4). Stakeholders referring to; "government, government civil agencies, the military, regulatory bodies, critical infrastructure (CI) operators, industry and businesses at large, small and medium enterprises (SME), research and development organizations, universities, individual citizens, and the population at large" (Luiijf E. B., Nineteen national cyber security strategies, 2013, p. 5). The purpose is to ensure the above stakeholders understand how the NCSS relates to other strategies such as; The national security and defence strategy, national digital agenda, and EU strategies such as the Digital agenda for Europe as an example. This approach will ensure the alignment of strategies and a

common direction for stakeholders. (Luiijf E. B., Nineteen national cyber security strategies, 2013, p. 5).

Six of the eight NCSS documents explicitly mention the countries national security strategy. Ireland implicitly refers to the national security by referring to the national risk assessment of 2014 and further discussed the negative consequences damage to critical infrastructure would have to national security. The NCSS does mention the relationships with the defence forces and outlines the role of the department of defence regarding cyber security in Ireland continuing to explain the role of An Garda Siochana in national security. All the NCSS documents explicitly discuss critical infrastructure as an important topic to protection. Ireland mentions the draft outline of the Network and Information Systems directive. Irelands NCSS predates the introduction of the NIS directive, May 2016. The later versions of strategies 2018, of the EU countries where the directive is applicable all mention protection of critical infrastructure as a key item to conform to.

The UK discusses protection of critical infrastructure however does not mention the NIS directive in its strategy. Ireland is the only country that refers to the EU digital agenda (2010). This may be an indicator of time lapse and relevance as nations now only refer to their own national digital agenda. Ireland's National Digital Strategy; "Doing More with Digital", was published in June 2013, focuses on increasing the extent and quality of online engagement. The UK similarly refers to its national digital agenda; 'the UK's Digital Strategy – the Government's digital ambition is for the UK to be the world's leading digital nation. In mentioning digital agendas, it is noteworthy to mention all nations discuss benefits of the digital economy and the prosperity and wealth cyber security can bring to national economies.

3.4.2 Addresses cyber threats

All the eight countries address in varying forms the cyber threats to nations' assets from critical infrastructures to social lives of citizens however rightly so, critical infrastructure is more explicitly discussed as opposed to citizen's social lives. The Canadian NCSS recognizes the changing landscape of cyber threats contributed by the advancement of digital technologies and emerging technologies. The NCSS refers to the extension of the threat landscape by the development of IoT applications such as, thermostats in homes, medical devices; pace makers to cars that all run on critical infrastructure and services. These intensives the need of protection for new cyber threats brought about by IoT. The UK similarly discusses threats by technology advancements referring as 'smart' systems; "Systems and technologies that underpin our daily lives – such as power grids, air traffic control systems, satellites, medical technologies,

industrial plants and traffic lights – are connected to the Internet and, therefore, potentially vulnerable to interference". (UK NCSS P. 13).

3.4.3 Threat subjects and malicious threat actor objectives

The UK and USA openly discuss cyber threats from other nations to national cyber security specifically mentioning potential attacks from foreign nations/cyber war to their country. The USA introduce their strategy mentioning the actions of competitors and adversaries to the fundamentals of cyber space the American vision of a "shared and open cyberspace for the mutual benefit of all" (USA). The USA and UK describe the development of tools to protect and retaliate if required against cyber-attacks, known as offensive cyber. The UK defines offensive cyber as; "Offensive cyber capabilities involve deliberate intrusions into opponent's systems or networks, with the intention of causing damage, disruption, or destruction". The Netherlands also acknowledge the development of national cyber tools "There has been an increase in the number of countries that are building offensive, military cyber capabilities" (NL NCSS). The Canadian NCSS acknowledges the actions of some nation states development of "advanced cyber tools with hostile aims" also mentioning terrorist's groups interests in advanced cyber tools to cause destruction.

Luxembourg is the only country that mentions the risk of technology mismatch "recurring errors made in the design or configuration of computer systems are the source of many problems related to information security". Luxembourg addresses this in objective three of their NCSS; requirement benchmarks and contractors. The USA discuss technology cyber threats from a procurement perspective and supply chain discussing the importance of national technology procurement.

Irelands strategy does not address or discuss threats in specifics as mentioned above in other NCSS documents. Irelands NCSS contains a section to 'Risks', section 2.3 however is limited to two paragraphs of high level content mentioning the rise of attacks and types of attacks as low level scale to high level mentioning criminal groups to nation states as responsible however no specific details mentioned. The second paragraph again mentions on a very high level the requirement to mitigate risks and closes with acknowledging Irelands complex set of risks based on the large number of data centric international companies based in Ireland.

3.5 Vision, Scope, Objectives and principles

3.5.1 National cyber security visions (Table 3)

According to (Luiijf E. B., Nineteen national cyber security strategies, 2013), a NCSS should present a "focal point at the horizon, a vision. Table 3 provides the visions mentioned by each of the countries either explicitly or implicitly. Security and resilience is explicitly mentioned as the vision of three nations; IRL, UK, Canada. However, six of the nation's mention securing and resilience as the vision where Luxembourg and Denmark take a different approach by vision is response mechanisms to risks and Denmark refer to manage of digital risks. Five of the eight nations mention either innovation, prosperity, digital solutions development and growth as its vision. Ireland provides a comprehensive vision to cyber security objectives in its vision more from a NCSS development aspect and not from an implementation perspective.

Table 3 - The National Vision of cyber security - IRELAND, UK, CANADA, USA, NETHERLANDS, DENMARK, LITHUANIA, LUXEMBOURG

	Country		2018
1	IRL	Explicit	Engage with a dynamic and challenging aspect of developments in digital technology, setting out the Government's approach to facilitating the resilient, safe and secure operation of computer networks and associated infrastructure used by Irish citizens and businesses. (IRL 2015)
2	UK	Explicit	Our vision for 2021 is that the UK is secure and resilient to cyber threats, prosperous and confident in the digital world.
3	CAN	Implicit	the Government of Canada and its partners will work together across three themes; Security and Resilience, Cyber Innovation, Leadership and Collaboration
4	USA	Implicit	Outlines how the United States will ensure the American people continue to reap the benefits of a secure cyberspace that reflects our principles, protects our security, and promotes our prosperity
5	NLD	Explicit	The Netherlands, together with her international partners, is committed to a secure and open cyber domain in which the opportunities offered to our society by digitalization are fully exploited, threats are mitigated, and fundamental rights and values are protected.
6	DEN	Explicit	Citizens, businesses and authorities must be familiar with and be able to manage digital risks, such that Denmark can continue to use digital solutions to support the development of the society.
7	LTU	Explicit	strengthening cyber security of the state and the development of cyber defence capabilities, at ensuring prevention and investigation of criminal offences committed using the objects of cyber security, at promoting the culture of cyber security and development of innovation, at enhancement of a close collaboration between public and private sectors as well as international cooperation and ensuring the fulfilment of international obligations in the field of cyber security in the country until 2023.

8	LUX	**Implicit**	full advantage is taken of new digital opportunities, while providing a response to the risks associated with ever-growing connectivity.

3.5.2 Strategic Objectives (Table 4)

Table 4 provides the strategic objectives outlined in each country respective NCSS. A summary review of the countries strategic objectives is outlined below table.

Table 4 - Strategic Objectives of the NCSS:
IRELAND, UK, CANADA, USA, NETHERLANDS, DENMARK, LITHUANIA, LUXEMBOURG

1	IRL	1	To improve the resilience and robustness of critical information infrastructure in crucial economic sectors, and particularly in the public sector.
		2	To continue to engage with international partners and international organizations to ensure that cyber space remains open, secure, unitary and free and able to facilitate economic and social development.
		3	To raise awareness of the responsibilities of businesses and of private individuals around securing their networks, devices and information and to support them in this by means of information, training and voluntary codes of practice.
		4	To ensure that the State has a comprehensive and flexible legal and regulatory framework to combat cyber-crime by An Garda Síochána that is robust, proportionate and fair, and that accords due regard to the protection of sensitive or personal data.
		5	To ensure that the regulatory framework that applies to the holders of data, personal or otherwise, is robust, proportionate and fair.
		6	To build capacity across public administration and the private sector to engage fully in the emergency management of cyber incidents.
2	UK	1	Defend - the UK against evolving cyber threats, to respond effectively to incidents, to ensure UK networks, data and systems are protected and resilient. Citizens, businesses and the public sector have the knowledge and ability to defend themselves.
		2	Deter - The UK will be a hard target for all forms of aggression in cyberspace. We detect, understand, investigate and disrupt hostile action taken against us, pursuing and prosecuting offenders. We have the means to take offensive action in cyberspace, should we choose to do so.
		3	Develop - We have an innovative, growing cyber security industry, underpinned by world leading scientific research and development. We have a self-sustaining pipeline of talent providing the skills to meet our national needs across the public and private sectors. Our cutting-edge analysis and expertise will enable the UK to meet and overcome future threats and challenges.
3	CAN	1	Secure and Resilient Canadian Systems
		2	An Innovative and Adaptive Cyber Ecosystem
		3	Effective Leadership and Collaboration
4	USA	1	Defend the homeland by protecting networks, systems, functions, and data
		2	Promote American prosperity by nurturing a secure, thriving digital economy and fostering strong domestic innovation
		3	Preserve peace and security by strengthening the United states ability - in concert with allies and partners - to deter if necessary punish those who use cyber tools for malicious purposes
		4	Expand American influence abroad to extend the key tenets of an open, interoperable, reliable, and secure internet.

5	**NLD**		The Netherlands is capable of capitalizing on the economic and social opportunities of digitalization in a secure way and of protecting national security in the digital domain.;
		1	The Netherlands has adequate digital capabilities to detect, mitigate and respond decisively to cyber threats
		2	International peace and security in the digital domain
		3	Digitally secure hardware and so ware
		4	Resilient digital processes and a robust infrastructure
		5	Successful barriers against cybercrime
		6	Cybersecurity knowledge development
		7	Public- private approach to cybersecurity
	DMK	**1**	Technological preparedness
		2	Raised awareness of cyber and information security among citizens, businesses and authorities
		3	Improved cooperation and coordination between responsible authorities.
	LTU	**1**	Strengthen cyber security of the country and the development of cyber defence capabilities.
		2	Ensure prevention and investigation of criminal offences in cyber space.
		3	Promote cyber security culture and development of innovation.
		4	Strengthen a close cooperation between private and public sectors
		5	Enhance international cooperation and ensure the fulfilment of international obligations in the field of cyber security
	LUX	**1**	Strengthening public confidence in the digital environment
		2	Digital Infrastructure Protection
		3	Promotion of the economy

Ireland provides six comprehensive strategic objectives mainly focusing on development of cyber strategy. Ireland does not provide any future vision and advantages of cyber security such as innovation and prosperity to the nation. The objectives are unstructured in comparison to the themes set out in the UK, USA, Canadian and Luxemburg strategies who put their strategic objectives into themes and pillars thus providing a clear direction to stakeholders. The USA, using pillars; Protect, Promote, Preserve and Influence. The Canadian theme; Security and Resilience, Cyber Innovation, Leadership and Collaboration. The UK focus on; Defend, Deter, Develop. Luxemburg's strategy is developed around three guidelines; Strengthen public confidence in the digital environment, protect digital infrastructures, Promote Luxembourg's economic position. Under each guideline there are several objectives to achieve the guideline. The Lithuanian strategy does not provide themes but covers the main objectives as; strengthening cyber security, development of cyber defence capabilities, prevention and investigation of criminal offences, promoting the culture of cyber security and development of innovation. Finally adding the enhancement of a close collaboration between public and private sectors as well as international cooperation. The UK, USA, Canada, heavily discuss the prosperity of the cyber security realm "Cyber security is becoming a driver of economic prosperity, and to determine the appropriate federal role in this digital age. (Government Of

Canada , 2019) with the US stating "Cyberspace has become fundamental to American wealth creation and innovation" and its fourth pillar 'Promote American Prosperity' dedicated to focusing on cyber benefits to the American economy and continuing to drive towards prosperity in its strategy. With the UK Chancellor of the Exchequer, MP Philip Hammond stating, "Much of our prosperity now depends on our ability to secure technology, data and networks from the many threats we face". (Add quote). The Netherlands also contribute to the advantages to be taken from the cyber security field stating; "The Netherlands is capable of capitalizing on the economic and social opportunities of digitalization in a secure way and of protecting national interests in the digital domain" The Netherlands outline a plan to achieve this via seven ambitions; "adequate digital capabilities to detect, mitigate and respond decisively to cyber threats, contributes to international peace and security in the digital domain, forefront of digitally secure hardware and software, resilient digital processes and a robust infrastructure, successful barriers against cybercrime, leads the way in the field of cybersecurity knowledge development, integrated and strong public-private approach to cybersecurity" (National Cyber Security Centrum , 2019).

3.5.3 Guiding Principles (Table 5)

Guiding principles can also be referred to as framework conditions. Table 5 provides the guiding principles of each country.

Table 5 Guiding principles of NCSS; IRELAND, UK, CANADA, USA, NETHERLANDS, DENMARK, LITHUANIA, LUXEMBOURG

1	**IRL (15)**	**1**	Rule of Law
		2	Subsidiarity
		3	Risk Based Approach & Proportionality
2	**UK**	**1**	Our actions and policies will be driven by the need to both protect our people and enhance our prosperity
		2	We will treat a cyber-attack on the UK as seriously as we would an equivalent conventional attack and we will defend ourselves as necessary
		3	We will act in accordance with national and international law and expect others to do the same
		4	We will rigorously protect and promote our core values. These include democracy; the rule of law; liberty; open and accountable governments and institutions; human rights; and freedom of expression
		5	We will preserve and protect UK citizens' privacy
		6	We will work in partnership. Only by working with the Devolved Administrations, all parts of the public sector, businesses, institutions, and the individual citizen, can we successfully secure the UK in cyberspace
		7	The Government will meet its responsibilities and lead the national response, but businesses, organizations and individual citizens have a responsibility to take

			reasonable steps to protect themselves online and ensure they are resilient and able to continue operating in the event of an incident
		8	Responsibility for the security of organizations across the public sector, including cyber security and the protection of online data and services, lies with respective Ministers, Permanent Secretaries and Management Boards
		9	We will not accept significant risk being posed to the public and the country as a whole as a result of businesses and organizations failing to take the steps needed to manage cyber threats
		10	We will work closely with those countries that share our views and with whom our security overlaps, recognizing that cyber threats know no borders. We will also work broadly across the range of international partners to influence the wider community, acknowledging the value of broad coalitions
		11	To ensure Government interventions are having a substantive impact on overall national cyber security and resilience, we will seek to define, analyse and present data which measures the state of our collective cyber security and our success in meeting our strategic goals
3	**Canada**	**1**	Protect the safety and security of Canadians and our critical infrastructure
		2	Promote and protect rights and freedom online
		3	Encourage cyber security for business, economic growth, and prosperity
		4	Collaborate and support coordination across jurisdictions and sectors to strengthen Canadas cyber resilience
		5	Proactively adapt to changes in the cyber security landscape and the emergence of new technology.
4	**USA**	**1**	Privacy and civil liberties need to be protected; Belief in the power of individual liberty
		2	Free Expression, Free markets, and privacy
		3	Commitment to the promise of an open, interoperable, reliable and secure internet to strengthen and extend our values and protect and ensure economic security for American workers and companies
5	**NLD**	**1**	Cyber security is an integral part of national security
		2	Public-Private Cooperation in the basis
		3	Government represents public interests, stimulates acceptance of own responsibilities and sets a good example
		4	Knowledge development and information sharing are crucial
		5	Mainstreaming of cybersecurity is a precondition
		6	The digital domain has no national borders
		7	Tension between interests require careful consideration
6	**Denmark**	**1**	The principle of sectoral responsibility; The authority which has day-to-day responsibility is also responsible in the event of a major accident or natural disaster.
		2	The similarity principle; The procedures and responsibilities that apply during normal day-to-day operations shall also, insofar as possible, apply in the crisis management system.
		3	The subsidiarity principle; The emergency response tasks must, insofar as possible, be managed locally and as close to the affected citizens as possible, and accordingly at the lowest suitable and relevant organisational level.

4	The principle of co-operation; Authorities have a separate responsibility for Collaborating and coordinating with other authorities and organisations about emergency response planning and crisis management.
5	The precautionary principle; In situations in which information is unclear or incomplete, the level of emergency preparedness should preferably be too High rather than too low. Furthermore, there should be possible to easily and quickly lower the level of emergency preparedness in order to prevent wasting resources.

Ireland provide three high level guiding principle statements that lack detail of the proposal of the national government toward cyber security for the nation. The principles are more statements of general rule such as law, responsibility, and identifying risk. The other countries explicitly refer to cyber threats with Ireland only mentioning cyber threats in principle number two; subsidiarity, where it mentions the state cannot assume sole responsibility. The Irish government should strengthen its guiding principles giving a stronger stance to cyber security and the intentions of the nation in protecting its citizens.

3.5.4 Stakeholders (Table 6)

Table 6 shows the stakeholders recognized in each countries NCSS. All the NCSS's expectantly refer to citizen's protection as a key stakeholder and state national security however not all countries explicitly mention small to medium enterprises or large organisations. Critical infrastructure operators have gained attention with all explicitly mentioning bar Ireland and UK who implicitly refer to operators.

Table 6 - The NCSS directly addresses the following types of stakeholders with respect to threats, vulnerabilities and measures

	Country	Citizens	SME	ISP	Large Organisations	CI Operators	The state /national security	Global infrastructure and issues
1	IRL	■	□	□	□	□	■	
2	UK	■		□	□	□	■	■
3	Canada	■	■			■	■	
4	USA	■	■	■	■	■	■	■
5	NDL	■	■	■	■	■	■	■
6	DEN	■	■	■	■	■	■	■
7	LIT	■	■	■	■	■	■	■
8	LUX	■	■	■		■	■	

Ireland should mention the role of key stakeholders in its strategy document to provide clarity the roles of stakeholders in cyber security. Ireland provides very little detail in relation to stakeholders and will need to explicitly mention in detail the roles of stakeholders in its revised and updated NCSS.

3.5.5 Key Actions (Table 7)

Table 7 illustrates the key action lines and planned actions by each of the eight countries as mentioned within their NCSS.

Table 7 - Key action lines and planned actions

Key actions and action lines	IRL	UK	CANADA	USA	NDL	DEN	LIT	LUX
Active/dynamic security measures		√		-	√	√	Item2 (Annex)	
Awareness and training/information security campaign	Objective 3	√	√	√	√	√	√	√
Adaptable policy to new ICT risk		√	√	√	√	√	√	√
Continuity and contingency plans			√	√	√	√	√	
Critical infrastructure protection	Objective 1	√	√	√	√	√	√	√
Cryptographic protection		Section (6.6)						
Cyber arms control		Section 6.5		√			√	
Defence cyber operations/intervention, training and exercises		√		√	√	√	Item1 (Annex)	
Develop and share good practices				√	√	√	√	
Develop and share good practices Economic growth	Objective 2			√	√	√	√	
Education and training	Section 5.10	√	√	√	√	√	Item4 (Annex)	
Exercises		√		√		√	√	
Explicit holistic view		√		√	√	√	√	
Exploitation to combat threats		√		√		√	√	
Improved security of ICT products		√	√	√	√	√		√
Information sharing/ exchange		√			√	√		
Intelligence gathering on threat actors		√		√	√	√		
International collaboration		√		√	√	√	Item21 (Annex)	
Legislation/legal framework	Objective 4	√		√	√	√		
Mandating security standards		√	√	√	√	√		Objective 4
National detection capability		√	√	√	√	√	Item5 (Annex)	√
National response capability/ICT crisis management	Objective 6	√	√	√	√	√		
Privacy protection	Objective 5	√		√	√	√		
Promote cyber-crime convention				√			Item19 (Annex)	
Protection of non-critical infra				√	√	√		
Public-private partnership				√	Objective 7	√	Item17 (Annex)	
Reducing adversary's motivation and capabilities		√		√	√	√		
Research and development		√	√	√	√	√		

Resilience against disturbances/threat and vulnerability reduction		√		√	√	√		√
Secure protocols and software		√		Pilar 1	√	√		
Secure sourcing of products		√		Pilar 1	√	√		
Self-protection of the government		√		√	√	√		
Strategic cyber security council					√	√		
Threat and vulnerability analysis		√	No	√	√	√		
Tracing criminals and prosecution		√	No	√	√		Item8 (Annex)	√
Actions defined Smartly?		Annex3					Annex	√

Of the above key action lines, Ireland actions are matched to the overall objectives in the strategy; critical infrastructure protection, develop and share good practices, awareness and training campaign, legal framework, privacy protection and national response. Irelands strategy does not provide any details on the action; how it will be actioned / carried out, responsible parties etc. Ireland does not outline the activities to be taken or elaborate on how the objectives are turned into actions.

The following summary paragraphs pertaining and summarising Key Actions look at the tactical/operational level plans as per (Luiijf E. B., Nineteen national cyber security strategies, 2013) framework. This research refers to the items for discussion in line with the nineteen strategies review.

SMARTness

(Luiijf E. B., Nineteen national cyber security strategies, 2013), posit the requirements and expectance of a NCSS to clearly define both tactical and operational actions in accordance to a specific, measurable, achievable, realistic and timely (SMART) manner. This approach will allow and assist governments to actively monitor completeness of objectives and success of delivery of actions outlined. It will also allow nations to gauge when and where insufficient action is taken to address the objectives of the strategy.

The Lithuanian NCSS includes an annex with tables of the 5 strategic objectives outlined in the NCSS and a set of actions to achieve each objective, assigning evaluation criteria for monitoring. The evaluation criteria hold three timeline values, initial value, 2021, and 2023, thus allowing monitoring of activities for completeness. The systematic approach of reporting by agencies on the implementation of the strategy is closely monitored and summarized in an Annual report on the state of National Security and Development. This approach could be

considered best practice as tasks are clearly defined and tracked. The UK's strategy also includes an Annex, Annex 3: Headline Implementation Programme. A table provides the desired strategic outcomes with corresponding indicative success measures up to 2021. The UK version is not as SMARTly defined with specific target measures as the Lithuanian strategy. The remaining strategies do not SMARTly define tasks.

Irelands strategy acknowledges the importance of Smartly defining tasks however does not appropriately deliver. The strategy references 'Risk Based Approach & Proportionality' as item three of its guiding principles with little description on how this will be implemented. The strategy outlines a number of key items to be achieved in the lifespan of the strategy but no specific or measurable actions nor monitoring for completion are defined.

Adaptability of future threats

Emerging technologies is widely recognized within the NCSS's as a future threat to cyber security. Technological advancement is enabling more and more items and people to be connected to the internet further exposing to risks of attack. Smart machines / systems, artificial intelligence, quantum computing, cloud computing, IoT are all increasing connectivity and exposing society to adversaries as the lines of physical and cyber world blur. The evolving nature of technology must be addressed within the security strategy to be relative to potential risks. Quantum computing, Artificial intelligence(AI), Internet of Things (IoT) are all technological developments that will impact nations and should be considered as part of the strategy. The Canadian strategy discusses the challenges to cyber security quantum computing poses to encryption also mentioning the use of blockchain technologies to secure government services. The strategy discusses various governmental initiatives to develop research and development in these areas. The USA also considers the impact of emerging technologies from a positive perspective "We will collaborate with the private sector and civil society to understand trends in technology advancement to maintain the United States technological edge in connected technologies and to ensure secure practices are adopted from the outset" (The Whitehouse, 2018).

Luxembourg specifies the need to consider the advancements of the digital economy stating, "the new cyber security strategy is aware of both the opportunities and risks which are inherent in new technologies" (The Luxembourg Government, 2018).

Ireland does not refer to technology but briefly mentions changes will be reflected in the strategy accordingly, "As events and technology continue to evolve, flexibility will be necessary and will be reflected in an adaptive and flexible implementation of the strategy. The adaptability of future threats also applies to the ever-greening process of reviewing the national cyber security strategy to ensure it reflects current trends in the threat landscape.

Planned actions in detail

Risk based assessment

The Netherlands publish annually a cyber security assessment namely "The Cyber Security Assessment Netherlands (CSAN) 2018". The CSAN is a publication of the National Coordinator for Security and Counterterrorism. The report is compiled by both the National Cyber Security Centre (NCSC), the Dutch Intelligence agency, with cooperation of the business community, government bodies and academia, with contribution from the business community, government bodies and academia. The report provides insights into threats, interests and resilience, as well as related developments in the field of cybersecurity, relevant for national security. (National Cyber Security Centrum Netherlands, 2019). Ireland discuss a risk based approach in their NCSS but do not implement any plan. "Measures to increase the level of protection need to be informed by an assessment of the risks and threats facing us, as individuals, businesses, public sector bodies and the State as a collective whole. Furthermore, such measures will need to be proportionate to the respective risks and threats that we face." Ireland does have a National Risk Assessment report carried out on an annual basis. The risk assessment does include a section on Technology with cyber security a key feature yearly. The National Risk Assessment and the National Cyber Security Strategy should be linked going forward.

Action plans and reporting

Canada intend to use cyber security action plans to supplement the strategy to bridge the gap of the evolving pace of cyber security advancements. The intention of the action plans is to "specify specific initiatives the government will undertake over time, with clear performance metrics and a commitment to report on results achieved" (Government Of Canada , 2019).

The United Kingdom's National cyber security strategy recognized from research collated by

(Shafqat & Masood, 2016) state "UK, USA and Germany particularly are better than the rest in terms of development and enforcement of action plans". The UK's strategy states "Activity to deliver the governments vision will advance the three primary objectives of the strategy: to defend our cyberspace, to deter our adversaries and to develop our capabilities". Defend, deter and develop are the key objectives of the UK's cyber strategy focusing on implementation.

Luxemburg's strategy is developed around three guidelines; Strengthen public confidence in the digital environment, protect digital infrastructures, Promote Luxembourg's economic position. Under each guideline there are a number of objectives defined to achieve the guideline, the implementation of the objectives will be accompanied by an action plan "outlining concrete measures to be implemented following a definite time frame, as well as actors called on to contribute to their implementation." (The Luxembourg Government, 2018).

3.5.6 NCSS Institutionalization

The Danish strategy, initiative 3.4, Strengthened national coordination, outlines the plan to set up a national steering committee for cyber and information security. The steering group will be responsible for the implementation and delivery of the strategy. In relation to a cyber-attack it is the principle of sectorial responsibility, this is the authority which "has the day to day responsibility is mentioned to have responsibility in the event of a major accident or disaster" Where there is a major cross-sectoral incidents other agencies such as the National Operative Staff, Danish National Police, Danish Defence Intelligence Service and Centre for Cyber Security will be called upon. The Danish strategy gives a detailed breakdown of the various agencies responsibilities within its strategy. The Luxembourg strategy mentions also the setting up by the government of an inter-ministerial coordination committee to sustain cybersecurity governance and facilitate the implementation of the NCSS objectives" (The Luxembourg Government, 2018, p. 10). For Canada, the government take the stance of having a clear visible leadership role. The Canadian government discuss the streamlining of ways of work and will establish clear focal points. The federal government will be responsible for development of national plans in conjunction with provinces, territories and private sector, to prevent and respond to cyber incidents. The USA confirm the implementation of their cyber security strategy is aligned with the National Security Strategy and therefore the national security council staff will coordinate with the various departments on implementing their NCSS.

In the review of the nineteen cyber security strategies 2013 it concluded that most of the 18 nation's national governments struggle with which governmental department or agency is the lead agency in the event of a major cyber-attack (Luiijf E. B., Nineteen national cyber security strategies, 2013). This has also been identified as the case for Ireland according to the Comptroller and Audit General findings who mention the steering group have only met up on one occasion since the creation of the group in 2015.

3.5.7 International Collaboration

Due to the global nature of cyberspace, international collaboration could be expected to be one of the highest priorities of each of the NCSS (Luiijf E. B., Nineteen national cyber security strategies, 2013). Also, a requirement of the NIS directive applicable to EU nations states is to engage and cooperation among all the Member States and the creation of CSIRT Networks (European Union , 2016).

3.6 Conclusion

The review and analysis of the chosen eight National cyber security strategies concludes that the appropriate level of understanding, commitment, appreciation and acknowledgement is presented by nations/governments of the potential threats and risks of cyber incidents to cyber security that exists. The review of the eight strategies highlighted the awareness among governments of the importance our digital resources and infrastructure plays in the modern world and the detrimental consequences of cyber sabotage. Governments are aware of the need for leadership in both protecting our digital economies and to maintain and develop the prosperity and wealth of the new digital economy. With greater global focus on cyber security the updating of strategies and the periods of revising strategy documents coincides with the attention cyber security has gained globally and the ever-changing landscape in technology reflects the requirement to revise documents frequently. The consciousness of the hazards that cyber threats can bring and the requirement for deterrence and resilience to cyber threats both from an end user to critical infrastructures is also addressed by the strategies. All the eight strategies mention resilience and deterrence of cyber threats across both the private and public sectors. Technological advancements, emerging technologies are also mentioned in most of the strategies whether it be the introduction of smart machines, IoT and quantum computing the acknowledgement by nations is we are continuing to live out more of our lives over the internet. The use of various technologies such as quantum and block chain could potentially

expose us to more incidents creating security concerns is cited too by the more technology focused strategies such as the UK strategy who mention specifically, cryptography. The requirement for strategies to follow a lifecycle methodology and clear SMART actions to ensure countries are continuously monitoring success and updating their strategies to reflect current and new cyber threats is a common theme among the strategies but only the Lithuanian strategy smartly defines objectives. Many of the countries have appointed inter-departmental oversight groups to monitor action plans pertaining to the cyber strategies. The awareness among nations that "digital innovation has become the engine of economic growth in the 21st century". Cyber security plays a vital role in the innovative growth as more and more emphasis is on securing digitalization to continue to grow and protect the integrity, availability and authenticity of digitalization. This cascades to research and development into innovation which also impacts the requirement for a skilled workforce in the cyber security field. "Cyber security is increasingly driving innovation and economic activity in Canada. It already contributes 1.7 billion to Canada's GDP and consists of over 11,000 well-paying jobs". (Government Of Canada , 2019). "A highly skilled cybersecurity workforce is a strategic national security advantage" (USA NCSS).

The lack of cyber security professionals is an issue globally with all the countries mentioned this in their strategies mentioning Canada confers this as an opportunity for Canada's "highly educated workforce". Luxemburg was ranked number one among 137 countries as part of an assessment of technological skills carried out by the world economic forum.

Finally, to go back to the beginning, the fundamentals on which the internet was born; Open, Free, and Secure Internet is currently being challenged by adversaries for criminality and cyber warfare. Some nations are now controlling and monitoring content citizens of nations can view, restricting websites and information bringing a new level to security on the web. The USA's deliberates on the evolution of cyber space in its introductory chapter reaffirming the vision for an open, interoperable, reliable, secure internet; "America's vision of a shared and open cyberspace for the mutual benefit of all". The USA mention specific adverse countries as; North Korea, Russia, Iran, who are challenging these fundamentals. The Canadian strategy states also advocates the vision of an open, free, and secure internet, working with international partners to advance Canadas interests. Ireland also refers explicitly to these fundamentals in both protection of citizen's fundamental human rights, protection of personal data by data protection legislation and ensuring the correct measures are in place is a prerequisite for open, free and safe access to cyberspace. (Department of Communications, Climate Action & Environment, 2015-2017). Ireland explicitly addresses cyber space remaining an open, secure

as an objective of its strategy stating; "To continue to engage with international partners and international organizations to ensure that cyber space remains open, secure, unitary and free and able to facilitate economic and social development." (Department of Communications, Climate Action & Environment, 2015-2017).

Overall Irelands strategy provides a high-level summary of key agenda items discussed at international level with little to no detail of how Ireland will implement its strategy and the direction of the nation. The strategy is at the development stage, outlining the requirements initially indicated by the EU cyber security strategy and the Network and Information systems Directive The strategy does not clearly identify stakeholders nor engage or inform the reader of the risks involved in cyber space. The strategy does not discuss the various threat actors or vectors. Advancements in technology is neither addressed or how the government will respond. In comparison to the other reviewed cyber security strategies Ireland is in the infinite stages of developing a national strategy. Ireland cyber security strategy requires immediate attention to protect the nation from cyber threats and fulfill the obligation of having a national strategy as currently there is no in-date strategy in place.

Chapter four will bring forward the main items of this research chapter to include in assisting Ireland to develop a revised National Cyber Security Strategy going forward.

Chapter Four: Discussions and Conclusions

4.0 Introduction

The purpose of this chapter is to appraise the key findings of the research. The chapter will summarize the conclusions of chapter three's review and analysis of National cyber security strategies developed by nations. The objective of the review was to compare findings to Ireland's efforts and provide recommendations for Ireland to strengthen both the national cyber security strategy and provide other initiatives that can assist Ireland in protecting the nation against cyber threats or provide better resilience. "This threat cannot be eliminated completely, but the risks can be greatly reduced to a level that allows society to continue to prosper and benefit from the huge opportunities that digital technology brings". (gov.uk , 2016).

This chapter will look at current developments and other reviews to date regarding Irelands undertakings to cyber security. The chapter will outline the status of cyber security activities and developments such as the findings from the Comptroller and Audit General report issued concerning the national cyber security and our obligations under EU law, most notably the transposition of the EU Network and Information Services (NIS) directive. The chapter will close with recommendations from the two chosen frameworks in assisting to develop, implement and maintain a NCSS.

The Department of Communications, Climate Action & Environment (DCCAE) is the responsible department for cyber security policy in Ireland. (Department of the Taoiseach, 2018). The DCCAE website refers to the published National Cyber Security Strategy 2015 as a "high level policy statement from government". The website further concludes the published documents key measures as, the establishment of the National Cyber Security Centre including the Computer Security Incident Response Team (CSIRT-IE), delivering improved security arrangements, introduction of primary legislation and co-operating with key agencies for the protection of critical infrastructure. The website briefly refers to the facilitation of education, training and public awareness initiatives. Finally concluding that an updated security strategy would be available in 2018. (Department of Communications, Climate Action & Environment, 2015-2017)

The 2018 revised version of a NCSS never transpired. The latest development as of the 19th March 2019 is the government is now calling for a public consultation to both public, private organizations, academia and citizens to contribute to the development of an updated National

Cyber Security Strategy. (Department of Communications Climate Action and Environment , 2019)

4.1 Background

Ireland published its first National Cyber Security Strategy in September 2015. The strategy is a high-level outline of the Irish governments proposed response to cyber threats and proposed security efforts. The strategy was reviewed in detail as part of Chapter three's analysis and review of published NCSS against two notable frameworks. The review allowed for comparison of Irelands efforts. The following sections highlight findings and where appropriate recommendations to assist Ireland in publishing a comprehensive strategy document with clear actions to strengthen Ireland's resilience to cyber threats.

4.2 Recent Developments

A number of recent developments relating to cyber security in Ireland are discussed in the following sections. The research disclosed an audit carried out by the Comptroller and Auditor General and details of the transposition of the NIS directive into Irish law. The review also highlighted cyber security as an item of the national risk assessments to date.

4.2.1 Report on the accounts of the public services

The Comptroller and Auditor General is the Irish government agency responsible for carrying out audits on public expenditure, resources and accountability. The agency conducted an audit of the National Cyber Security Centre in 2018. The examination by the Comptroller and Auditor General reviewed the progress of the National Cyber Security Centre, the 2015 National Cyber Security Strategy and the transposing of the EU Network and Information Systems Directive. The report reviewed the strategic direction of the Centre in the context of the requirements set out in the EU directive, its cost, resourcing and the governance and oversight arrangements in place". (Office of the Comptroller and Audit General, 2018). The Comptroller assessment refers to an accompanying implementation plan to the National cyber security strategy. This document does not appear to have been available publicly as no document could be found for this research.

The Comptroller Auditor report includes a progress assessment of the National Cyber Security Strategy Assessment and mention it is combined with the implementation plan. The

assessment measures are as outlined in chapter 5. 'Measures' in the 2015-2017 National Cyber Security Strategy. The progress assessment status by the Comptroller is as of May 2018. Of the twelve measures outlined the Comptroller report concluded four were completed during the period of 2015 until May 2018.

The twelve measures and status as of May 2018 are as follows;

Measure	Status
Establish the National Cyber Security Centre (NCSC) within the Department	Completed
Network and Information Security for public bodies	Partial progress
Coherent international engagement	Completed
Fully implement the EU Directive by primary legislation	Not Completed
National security and policing	Not Completed
Cybercrime	Not Completed
Civil-military cooperation	Completed
Protection of critical national infrastructure	Partial progress
Information sharing	Completed
Education and training	Partial progress
Public awareness	Partial progress
Relationship with third level institution	Not complete

Under each of the measures above there are actions / sub items for completion for each measure. The report into the findings on the operations of the National Cyber Security Centre are summarized as; having no strategic plan, funding concerns and the absence of the oversight body of the centre who have not met since 2015. (The Irish Times , 2018). The centre was set up in 2011, reporting to the Department of Communications, Climate Action and Environment (DCCAE). The Computer Security Incident Response Team (CSIRT) is also located at the centre which is situated in rented accommodation of UCD, university campus. The audit was to review the progress made by the centre since its establishment. The findings included the lack of resourcing of the centre albeit the government approved funding of 800,000 a year to resource the centre however between the period of 2012-2015 only a third of allocated funding was used. In 2017, the allocation increased to 1.95 million. The agency response to the Comptroller for the reasoning behind the increased spend of funding, the department responded stating that the challenges previously was with understanding the skills of resources required. (Office of the Comptroller and Audit General, 2018).

4.2.2 Government National Risk Assessments

The Department of the Taoiseach conduct an annual National Risk Assessment. The assessment has been carried out since 2014. The National Risk Assessment aim is to identify the strategic risks to Ireland's future wellbeing that face the country over the medium and long term. The National Risk Assessment is published annually after a draft issue and public consultation period before the final version is released. The government state the risk assessment is "an opportunity to take a bird's eye view of the biggest risks facing the country." (Department of the Taoiseach, 2019). The assessment identifies risks under headings: geopolitical, economic, environmental, social and technological. The assessment aims to increase awareness and provide a framework for departments to consider mitigation actions and plans. (Department of the Taoiseach, 2019). Since its creation in 2014 cyber security has remained a prominent risk identified to the nation.

Technological Risks Cyber Security

The 2018 National Risk Assessment, Chapter 6 is dedicated to Technological Risks. For the fourth year running cyber security is declared as a national strategic risk. The assessment states two cyber security risks as; the disruption to critical infrastructure and data fraud and theft as strategic risks. Disruption to critical infrastructure and services as a significant risk and mentions IoT as an enabler to cyberattacks. The assessment also discusses the threat actors as both state and non-state actors and motivations for attack. Cyber criminals and organized crime using the WannaCry attack as an example to the motives of criminal gangs to hold organisations to ransom, the risk associated been financial and reputational.

"Europol currently judges the risk of cyber-terrorism to be one of high potential but low probability, though the probability may be increasing. This is an issue of growing concern at EU and international levels reflecting the importance of continuing to build our expertise and capacity in cyber security to enable us to address these threats effectively."

The second risk of Cyber Security is 'Data fraud and theft'. Discussing how the internet is a key enabler for economic growth and prosperity leads to the position of Ireland "any challenge to the quality of Ireland's data regulation environment, which has been key to the continuing expansion and growth of the digital economy in Ireland, creates a risk of business disruption as well as reputational damage."

Skilled Cyber Security Workforce

Ireland has also acknowledged and acted on this issue by The Industrial Development Authority (IDA) agreeing to fund a new cyber security cluster based in Cork with the aim of putting Ireland on the map for cyber security expertise. This is the first time the Irish state has funded an initiative such as this. (The Irish Times , 2018). This development is a step in the right direction for Ireland to compete in the prosperous environment cyber security can bring as outlined by other countries strategies when mentioning the benefits to cyber security for national prosperity and wealth.

4.3 Recommendations

4.3.1 National Cyber Security Strategy Draft Public Consultation

19th March 2019 (MerrionStreet.ie, 2019), releases a governmental statement "Minister Bruton Opens Public Consultation on a new National Cyber Security Strategy". The minister for Communications, Climate, Action and Environment, Mr. Richard Burton has called for responses to ten specific questions pertaining to cybersecurity in Ireland. Questions are attached as Appendix One.

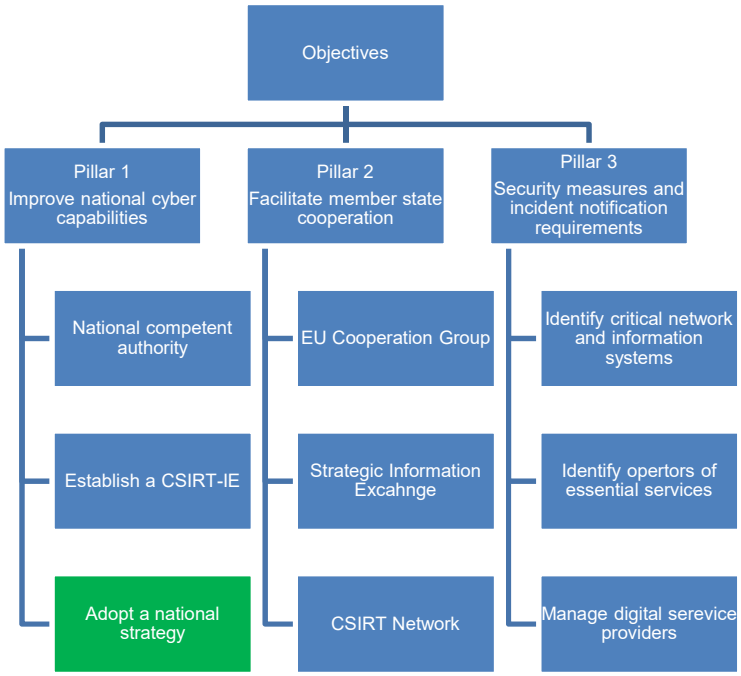
This approach taken by the Irish government follows suit to other countries successful 'call for comments'. The Canadian government held public consultation into the development of their 2018 NCSS with over 2,000 submissions. Canada frequently refer to comments from both public, private, academia in their NCSS document making the strategy more relatable to both citizens and SME's. This will benefit and enhance Irelands revised strategy as the previous strategy provides little to no stakeholder analysis or engagement. New Zealand have taken a similar approach; The New Zealand government speak of its 2015 version of its cyber security strategy as an overarching document where now it wants to focus on a more measured approach similar to both the UK and Australia, this should be the approach Ireland takes in its 2019 strategy. From the consultation request for Ireland a set of draft guidelines with ten questions gives us an indication Ireland intends to follow a similar approach by outlining pillars of interest as strategic objectives for Ireland; Protect, Develop, Engage. The questions of the draft guidelines consultation are below and will allow us to provide our conclusive observations to answer.

The DCCAE is "responsible for coordinating the governmental emergency response to any national-level cyber security incidents. The Department discharges these responsibilities

through the National Cyber Security Centre". (Office of the Comptroller and Audit General, 2018). Fianna Fail TD Jack Chambers discussed with the Minister of Defence, Paul Kehoe what the role the Department of Defence plays in national cyber security suggesting the department of defence should take a lead governing role rather than the department of communications as cyber is no longer a technological issue but one of national security. (Kildare Street , 2018).

4.3.2 NIS Directive

The Network and Information Systems Directive was transposed into Irish law on the 18th September 2018. The directive ensures a minimum set of standards to cyber security for EU member countries. The transposition of the directive into Irish law ensures Ireland upholds a minimal level of security and conforms to the objectives of the directive as outlined below. By complying to the objectives of the law will ensure protection to Irelands cyber space and international engagement.



Article 7 of the NIS directive specifies the following seven issues that should be part of a member states NCSS.

a) The objectives and priorities of the national strategy on the security of network and information systems;
b) A governance framework
c) Identification
d) Indication of the education
e) Research and development
f) Risk assessment plan
g) List of various actors

The directive is a good benchmark overall for the objectives Ireland should aim to manage in general for overall cyber security and not just in critical sectors. On a national level the objectives can be implemented.

4.3.3 ENISA Analysis

The ENISA framework analysis concluded Ireland delivered the least number of objectives set out in the ENISA good practice user guide reaching five out of the fifteen objectives provided by the agency. The new version of the NCSS should review and include Ireland's position on all the fifteen objectives as outlined by ENISA. The research has discovered Ireland has taken measures to some of the objectives however the NCSS policy document does not reflect this. The NCSS should act as an informative document on all national cyber security initiatives. Defining actions in a SMART measure will clearly determine if there are gaps in objectives.

4.3.4 Nineteen Strategies

(Luiijf E. B., Nineteen national cyber security strategies , 2013), strongly recommend the defining of the term 'cyber security' in a NCSS. (Luiijf E. B., Nineteen national cyber security strategies , 2013) discuss the reasons for this is to set a common ground and will allow better communications, engagements and understandings internationally of the scope of cyber security been referred to. The identification of threats, threat actors, relationships with other policy documents, clear strategic direction are all recommended in the nineteen strategies review.

From examples of other strategies, a themed approach to strategic objectives is very useful to clearly state the objectives. This appears to be a similar direction that will be taken by the new version of Irelands NCSS based on the draft consultation paper where the following themes are mentioned; Protect, Develop and Engage.

Further recommendations

It is recommended Ireland should follow the lifecycle approach for its cyber security strategy. From the 2015 Ireland NCSS document it would indicate Ireland is at Phase 1 in the cycle with no clear documentation outlining phases 2-3. Ireland should focus on Phase 2 in 2019 documenting the execution of cyber security activities followed by the remaining phases; evaluation and maintaining to continue the cycle. The lifecycle approach is briefly described below.

Lifecycle Approach

The ENISA user guide recommends the use of a NCSS Lifecycle approach that will allow nations to check and continuously improve the strategy (ENISA, 2019). (Shafqat & Masood, 2016) support the continuous revising of the security strategy stating, "the continuously changing spectrum of cyber threats has made it imperative to update the cyber security strategy to encompass emerging threats and relevant countermeasures". The lifecycle developed by ENISA outlines phases for governing national cyber security strategies. There are four phases outlined;

Phase 1 - Developing the strategy
Phase 2 - Executing the strategy
Phase 3 - Evaluating the strategy
Phase 4 - Maintaining the strategy

(ENISA, 2019)

4.4 Conclusion

From the research conducted it appears Ireland has significantly upped its game within the cyber security realm in the past two years. The approach seems slow and sporadic but nevertheless a structured approach with the recently new developments of the draft public consultation note to a revised National Cyber Security Strategy and other initiatives outlined indicate a move in the right direction of responding to the risks of cyber security. The NCSS draft outline presents a lot of the recommended best practice approaches this research has found. Ireland is without a Cyber security strategy since the end of 2017 with government informing a new version would be available from 2018. The call for consultation deadline is 1st

May 2019. The paper states a review team will look at the responses. With an outline of ten questions calling to all of society and from examples of previous countries consultation a large volume of responses was received, late 2019 could be optimistic for turnaround. If this is the case Ireland is at risk of exposing itself to cyber threats and missing the opportunities that can be had by leading a cyber security nation. Ireland needs to act fast in this ever-changing landscape and keep the momentum to both secure ICT and to potentially benefit from cyber security.

Interestingly, the Comptroller General assessment dated as of May 2018 closed 4 measures as complete out of twelve measures outlined in the 2015-2017 strategy. Remarkably the draft consultation paper for the new NCSS, chapter 2 refers to all the measures stated in the previous NCSS as now all items fully completed. The actions form Chapter 2 of the Draft Public Consultation document and list all items as been complete with a description of each action taken.

Both the ENISA and Nineteen strategies review conclude Ireland needs to include more concrete detailed plans to its new revised NCSS. The ENISA framework review highlighted Ireland had implemented the least number of objectives out of the twenty-eight EU countries, mentioning only five out of fifteen. The nineteen strategies framework review similarly highlighted areas for improvement for Ireland to build a comprehensive, complete guiding and informative strategy to cyber security.

Appendix 1: National Cyber Security Strategy Draft Public Consultation

Ten questions;

1. Having regard to the developing challenges and risks arising in cyber security, and the progress made as outlined in the draft consultation document, what should be the focus and key objectives of this Strategy?

Protect

2. Are further steps/measures required to protect critical national infrastructure, including those sectors outside of those covered by the NIS Directive?
3. In relation to meeting the threats posed to integrity of the electoral process, what are the key Cyber Security measures that should be taken, and how might these contribute to the national response to hybrid threats?
4. Government IT systems are owned and operated by a wide range of operators; what measures should be taken to ensure that public services and data are secured to a uniform and high degree, with reference to governance, staffing, organization and training?
5. Are public information campaigns focused on general messages around online fraud and phishing attacks aimed at individuals useful, or should the focus of public information campaigns be on measures designed to assist small and medium businesses in mitigating risks to their businesses and data, or are both issues equally important?

Develop

6. What are the key challenges initiatives and measures are required to develop the Irish cyber security industry, with particular regard to supporting the research and development agenda?
7. What kind of measures could be undertaken by Government to improve the availability of skilled workers in this field?
8. How might the relationship between academia and industry be facilitated to ensure that third level institutions are providing and developing the skills that industry require?

Engage

9. What concrete structures can be put in place so that developments in Cyber Security community (industry, academia and prospective workers in the area) are clearly understood by Government, and vice versa?
10. What role should the State play in the international discussion around Cyber Security, responsible State and non-State behavior, and the responsibilities of private industry?

References

Damien McGuinness, 2017. *How a cyber attack transformed Estonia.* [Online]
Available at: http://www.bbc.com/news/39655415
[Accessed 10 May 2018].

Aggarwal, G., 2015. *General Awareness on CyberCrime ,* Punjab, India : International Journal of Advanced Research in Computer Science and Software Engineering.

Allison, P. R., 2016. Cyber Security. *What EU's Cyber Security Bill means for UK Industry* , 23 February , pp. p21-26.

Allison, P. R., 2017. Computer Weekly. *Organised crime exploiting new technology: European law enforcement is collaborating with industry around cyber crime as study shows that organised crime groups increasingly exploit new technologies*, 27 June, pp. p19-23.

Allison, P. R., 2017. Cyber Crime. *Criminals in the machine*, 3 July, pp. 19-23.

Biography , 2018. *Edward Snowden.* [Online]
Available at: https://www.biography.com/people/edward-snowden-21262897
[Accessed 20 May 2018].

Caldwell, T., 2017. *Science Direct.* [Online]
Available at: https://www.sciencedirect.com/science/article/pii/S1361372317300246
[Accessed 10 09 2018].

Commission, E., 2013. *EU Cybersecurity Strategy.* [Online]
Available at: https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-strategy
[Accessed 01 May 2018].

Council Of Europe, 2018. *Budapest Convention and Related Standards.* [Online]
Available at: https://www.coe.int/en/web/cybercrime/the-budapest-convention
[Accessed 20 May 2018].

Craigen , D., Diakun-Thiabault, N. & Purse , R., 2014. Defining Cybersecurity. *Technology Innovation Management Review,* pp. 13-21.

Data Protection Commission , 2018. *Data Protection.* [Online]
Available at: https://dataprotection.ie/docs/What-is-Personal-Data/m/210.htm
[Accessed 10 May 2018].

Data Protection Commission , 2018. *GDPR and You.* [Online]
Available at: http://gdprandyou.ie/individuals/
[Accessed 01 May 2018].

Department of Communications Climate Action and Environment , 2018. *National Cyber Security Strategy.* [Online]
Available at: https://www.dccae.gov.ie/en-ie/communications/topics/Internet-Policy/cyber-security/national-cyber-security-strategy/Pages/NCSC-Strategy.aspx
[Accessed 11 February 2018].

Department of Communications Climate Action and Environment , 2019. *National Cyber Security Strategy Public Consultation.* [Online]
Available at: https://www.dccae.gov.ie/en-ie/communications/consultations/Pages/2019-National-Cyber-Security-Strategy.aspx
[Accessed 19 March 2019].

Department of Communications, Climate Action & Environment , 2019. *National Cyber Security Strategy.* [Online]
Available at: https://www.dccae.gov.ie/en-ie/communications/topics/Internet-Policy/cyber-security/national-cyber-security-strategy/Pages/NCSC-Strategy.aspx

Department of Communications, Climate Action & Environment, 2015-2017. *National Cyber Security Strategy.* [Online]
Available at: https://www.dccae.gov.ie/en-ie/communications/topics/Internet-Policy/cyber-security/national-cyber-security-strategy/Pages/NCSC-Strategy.aspx

Department of the Taoiseach, 2018. *gov.ie.* [Online]
Available at: https://assets.gov.ie/2275/241018133005-79185c8804314719bc9656328a460308.pdf
[Accessed 10 February 2019].

Department of the Taoiseach, 2018. *National Risk Assessment 2017 Overview of Strategic Risks.* [Online]
Available at: https://assets.gov.ie/2275/241018133005-

79185c8804314719bc9656328a460308.pdf
[Accessed 10 February 2019].

Department of the Taoiseach, 2019. *gov.ie.* [Online]
Available at: https://www.gov.ie/en/news/d7281a-government-publishes-the-national-risk-assessment-2018/
[Accessed 10 February 2019].

Department of the Taoiseach, 2019. *Government publishes the National Risk Assessment 2018.* [Online]
Available at: https://www.gov.ie/en/news/d7281a-government-publishes-the-national-risk-assessment-2018/
[Accessed 10 February 2019].

Dixon , Hayley; Swinford , Steven; Majid, Aisha;, 2018. *Hackers 'led warplanes to Syrian hospital' after targeting British surgeon's computer.* [Online]
Available at: https://www.telegraph.co.uk/news/2018/03/20/british-surgeon-helped-syrian-operations-hacked-reveal-secret/
[Accessed 10 May 2018].

ENISA , 2019. *National Cyber Security Strategies (NCSSs) Map.* [Online]
Available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map

ENISA , 2019. *ncss-good-practice-guide.* [Online]
Available at: https://www.enisa.europa.eu/publications/ncss-good-practice-guide

ENISA, 2018. *About ENISA.* [Online]
Available at: https://www.enisa.europa.eu/about-enisa
[Accessed 10 December 2018].

ENISA, 2018. *Looking into the crystal ball A report on emerging technologies and security challenges,* Athens : ENISA .

EU GDPR , 2018. *GDPR Key Changes.* [Online]
Available at: https://www.eugdpr.org/key-changes.html
[Accessed 01 May 2018].

European Commission , 2018. *Cyber Security.* [Online]
Available at: https://ec.europa.eu/digital-single-market/en/cyber-security
[Accessed 14 Febraury 2019].

European Commission , 2019. *The Cybersecurity Act strengthens Europe's cybersecurity.* [Online]
Available at: https://ec.europa.eu/digital-single-market/en/news/cybersecurity-act-strengthens-europes-cybersecurity
[Accessed 20 April 2019].

European Commission, 2010. *A Digital Agenda for Europe.* [Online]
Available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF
[Accessed 14 November 2018].

European Parliment, 2019. *Legislative Train Schedule Connected to the Digital Market.* [Online]
Available at: http://www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market/file-cyber-security-package
[Accessed 01 May 2019].

European Union , 2016. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. *Official Journal of the European Union,* Issue OJ L 194, pp. 1-30.

European Union, 2018. *European Union.* [Online]
Available at: https://eeas.europa.eu/headquarters/headquarters-homepage/search/site/JOINT%20COMMUNICATION%20TO%20THE%20EUROPEAN%20PARLIAMENT%2C%20THE%20COUNCIL%2C_en
[Accessed 8 April 2018].

Europe, C. o., 2001 . *Convention on Cybercrime.* [Online]
Available at: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf
[Accessed 30 April 2018].

Europol, 2014. *The Internet Organised Crime Threat Assessment (iOCTA).* [Online]
Available at:
http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/europol_iocta_/europol_iocta_en.pdf
[Accessed 10 May 2018].

Europol, 2018. *Internet Organised Crime Threat Assessment 2018.* [Online]
Available at: https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018
[Accessed 01 April 2019].

Gervais, M., 2012. Cyber Attacks and the Laws of War. *Berkeley J. Int'l L. 525 (,* pp. 525-579.

gov.uk , 2016. *National Cyber Security Strategy 2016 to 2021.* [Online]
Available at: https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021
[Accessed 10 February 2019].

GOV.UK, 2016 . *National Cyber Security Strategy 2016 to 2021.* [Online]
Available at: https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021
[Accessed 01 December 2018].

Government Of Canada , 2019. *National cyber security strategy : Canada's vision for security and prosperity in the digital age.* [Online]
Available at: http://publications.gc.ca/site/eng/9.856424/publication.html

Government of the Netherlands , 2018. *Forms of Cybercrime.* [Online]
Available at: https://www.government.nl/topics/cybercrime/forms-of-cybercrime
[Accessed 01 May 2018].

Greenberg, A., 2017. *How An Entire Nation Became Russia's Test Lab for Cyberwar.* [Online]
Available at: https://www.wired.com/story/russian-hackers-attack-ukraine/
[Accessed 06 May 2018].

Greenemeire, Larry, 2015. *A Quick Guide to the Senate's Newly Passed Cybersecurity Bill.* [Online]
Available at: https://www.scientificamerican.com/article/a-quick-guide-to-the-senate-s-newly-

passed-cybersecurity-bill/
[Accessed 01 May 2018].

Haataja, S., 2017. The 2007 cyber attacks against Estonia and international law on the use of force: an informational approach. *Law, Innovation & Technology,* 9(2), pp. 159-189.

Halder, D. & Jaishankar, K., 2011. *Cyber crime and the victimization of women: Laws, Rights and Regulations.* 1 ed. Hersey, PA, USA: IGI Global.

Interpol, 2018. *Cybercrime.* [Online]
Available at: https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime
[Accessed 01 May 2018].

Interpol, 2018. *INTERPOL-Europol conference calls for global response to cybercrime.* [Online]
Available at: https://www.interpol.int/News-and-Events/News/2018/INTERPOL-Europol-conference-calls-for-global-response-to-cybercrime
[Accessed 10 January 2019].

ITU , 2019. *About International Telecommunication Union (ITU).* [Online]
Available at: https://www.itu.int/en/about/Pages/default.aspx
[Accessed 10 January 2019].

Keen, A., 2018. *Where in the world will you find the most advanced e-government? Estonia..* [Online]
Available at: https://ideas.ted.com/where-in-the-world-will-you-find-the-most-advanced-e-government-estonia/
[Accessed 17 March 2018].

Kildare Street , 2018. *Dail Debates.* [Online]
Available at: https://www.kildarestreet.com/debates/?id=2018-10-03a.89
[Accessed 01 March 2019].

Klimburg, A., 2012. *National Cyber Security Framework Manual,* Tallinn: NATO CCD COE Publication.

Kovacs, L., 2018. Cyber Security Policy and Strategy in the European Union and Nato. *Military Art and Scines,* 89(1), pp. 16-24.

Lachow, I., 2011. The Stuxnet Enigma: Implications for the Future of Cybersecurity. *11 Geo. J. Int'l Aff,* Volume 11, p. 118.

Luiijf, E. B. K. &. D. G. P., 2013 . Nineteen national cyber security strategies. *International Journal of Critical Infrastructures,* pp. 6, 9(1-2), 3-31..

Luiijf, E. B. K. &. D. G. P., 2013. Nineteen national cyber security strategies. *International Journal of Critical Infrastructures,* pp. 6, 9(1-2), 3-31..

Luiijf, H. B. K. S. M. a. D. G. P., 2011. Ten national cyber security strategies: A comparison. *International Workshop on Critical Information Infrastructures Security ,* September .pp. 1-17.

MerrionStreet.ie, 2019. *Minister Bruton Opens Public Consultation on a new National Cyber Security Strategy.* [Online]
Available at: http://merrionstreet.ie/en/News-Room/Releases/Minister_Bruton_Opens_Public_Consultation_on_a_new_National_Cyber_Security_Strategy.html

National Cyber Security Centrum , 2019. *National Cyber Security Agenda.* [Online]
Available at: https://www.ncsc.nl/english/current-topics/national-cyber-security-agenda.html

National Cyber Security Centrum Netherlands, 2019. *Cyber Security Assessment Netherlands CSAN 2018.* [Online]
Available at: https://english.nctv.nl/binaries/CSBN2018_EN_web_tcm32-346655.pdf

North Atlantic Treaty Organisation , 2018. *Cyber Defense.* [Online]
Available at: https://www.nato.int/cps/en/natohq/topics_78170.htm
[Accessed 14 February 2019].

Office Of The Comptroller & Auditor General, 2017. *2017 Annual Report, Chapter 08: Measures relating to national cyber security.* [Online]
Available at: https://www.audit.gov.ie/en/Find-Report/Publications/2018/2017-Annual-Report-Chapter-08-Measures-relating-to-national-cyber-security.pdf
[Accessed 10 January 2019].

Office of the Comptroller and Audit General, 2018. *Office of the Comptroller and Audit General.* [Online]
Available at: https://www.audit.gov.ie/en/Find-

Report/?keyword=cyber+&sectors=Communications&topics=Governance&years=-1
[Accessed 10 February 2019].

Official Journal of the European Union , n.d. *Directive (EU) 2016/1148,* s.l.: s.n.

Oxbridge Essays, 2017. *How to do your dissertation secondary research in 4 steps.* [Online]
Available at: https://www.oxbridgeessays.com/blog/how-to-dissertation-secondary-research-4-steps/#thebasics
[Accessed 22 April 2019].

Oxford Dictionaries, 2018. *Cyberattack.* [Online]
Available at: https://en.oxforddictionaries.com/definition/cyberattack
[Accessed 01 May 2018].

Pernik, P., 2014 . Improving cyber security: NATO and the EU. *International centre for defence studies,* pp. 1-20.

Redpacket Security , 2016. *Stuxnet : Operation Olympic Games NSA Codename.* [Online]
Available at: https://www.redpacketsecurity.com/stuxnet-operation-olympic-games-nsa-codename/
[Accessed 17 March 2019].

Reuters, 2017. *Ukraine's power outage was a cyber attack: Ukrenergo.* [Online]
Available at: https://www.reuters.com/article/us-ukraine-cyber-attack-energy/ukraines-power-outage-was-a-cyber-attack-ukrenergo-idUSKBN1521BA
[Accessed 10 April 20178].

RTE News, 2018. *So you think you know about cybercrime.* [Online]
Available at: https://www.rte.ie/eile/brainstorm/2018/0210/940055-so-you-think-you-know-about-cybercrime/
[Accessed 2018 April 09].

Senker, C., 2017. *CyberCrime and the Darknet Revealing the hidden underworld of the internet.* 1 ed. London : Arturus Publishing Limited/Cath Senker.

Shafqat, N. & Masood, A., 2016 . Comparative Analaysis of Various National Cyber Security Strategies. *International Journal of Computer Science and Information Security ,* pp. 129-136.

Singer, P., 2015. Stuxnet and its hidden lessons on the ethics of cyberweapons.. *Case W. Res. J. Int'l ,* Volume 47, p. 79.

Statista, 2018. *Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions).* [Online]
Available at: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/
[Accessed 06 May 2018].

Steven Cherry, 2011. *Sons of Stuxnet.* [Online]
Available at: https://spectrum.ieee.org/podcast/telecom/security/sons-of-stuxnet
[Accessed 10 March 2019].

Štitilis, D. P. P. a. M. I., 2017. EU and NATO cybersecurity strategies and national cyber security strategies: a comparative analysis. *Security Journal ,* Volume 30(4), pp. 1151-1168.

Swire, P., 2018. A Pedagogic Cybersecurity Framework: A proposal for teaching the organizational, legal, and international aspects of cybersecurity. *Communications of the ACM,* 61(10), p. 23–26.

Techopedia, 2018. *Cyber Attack.* [Online]
Available at: https://www.techopedia.com/definition/24748/cyberattack
[Accessed 01 May 2018].

TechTarget, 2018. *TechTarget.* [Online]
Available at: https://searchsecurity.techtarget.com/definition/cybersecurity
[Accessed 10 October 2018].

TechTarget, n.d. *Cybercrime.* [Online]
Available at: https://searchsecurity.techtarget.com/definition/cybercrime
[Accessed 12 May 2018].

The Council on Foreign Relations, 2019. *Cyber Operations Tracker.* [Online]
Available at: https://www.cfr.org/interactive/cyber-operations
[Accessed 6 May 2019].

The Irish Times , 2018. *Cyber security unit has no strategic plan, C&AG finds.* [Online]
Available at: https://www.irishtimes.com/news/ireland/irish-news/cyber-security-unit-has-no-strategic-plan-c-ag-finds-1.3645150

The Irish Times , 2018. *IDA to fund new cybersecurity cluster to put Ireland on global map.* [Online]

Available at: https://www.irishtimes.com/business/technology/ida-to-fund-new-cybersecurity-cluster-to-put-ireland-on-global-map-1.3728777

United Nations Office of Disarment Affairs , 2018 . *Developments in the field of information and telecommunications in the context of international security.* [Online]
Available at: https://www.un.org/disarmament/ict-security/
[Accessed 14 November 2018].

Whitson, G., 2013. *Cybercrime.* [Online]
Available at: http://eds.b.ebscohost.com.elib.tcd.ie/eds/detail/detail?vid=0&sid=3de2dd3d-762e-4b7b-9c3f-1619648feacd%40sessionmgr104&bdata=JnNjb3BlPXNpdGU%3d#AN=89138922&db=ers
[Accessed 10 April 2018].

Wikipedia, 2018. *Cyber Crime.* [Online]
Available at: https://en.wikipedia.org/wiki/Cybercrime
[Accessed 10 April 2018].

World Economic Forum, 2018. *Billions of devices will soon be vulnerable to cyberattack. But we're not ready.* [Online]
Available at: https://www.weforum.org/agenda/2018/03/how-will-new-cybersecurity-norms-develop
[Accessed 17 March 2019].

World Economic Forum, 2018. *Billions of devices will soon be vulnerable to cyberattack. But we're not ready.* [Online]
Available at: https://www.weforum.org/agenda/2018/03/how-will-new-cybersecurity-norms-develop
[Accessed 17 March 2019].