What Impact Does Cybersecurity Have on Bolstering or Eroding the National Resilience of Estonia?  
May 2018  
Glasgow Student Number: 2280334  
Charles Student Number: 11375418  

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

Word Count: 20,376  
Supervisor UofG: Dr Luca Anceschi  
Supervisor Charles Uni: Dr Vit Stritecky
MSc International Security, Intelligence and Strategic Studies  
2017-2019

Dissertation Archive Permission Form
I give/do not give [please delete as appropriate] the School of Social and Political Sciences, University of Glasgow permission to archive an e-copy/soft-bound copy of my MSc dissertation in a publicly available folder and to use it for educational purposes in the future.

Student Name (BLOCK LETTERS): ________________________________

Student Number: ________________________________

Student Signature: ____________________ Date: ____________________

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

I would like to express my gratitude towards my advisors Dr Luca Anceschi and Dr Vit Stritecky. My mother, Ailsa M. Wilson, QC, deserves a very special thanks as without her continued and undivided support this thesis would not be possible. Also, Erin Duncan’s patience and support has been truly invaluable.
ABSTRACT

This thesis is an attempt to analyse the relationship between the increasingly popular concept of national resilience and cybersecurity. National resilience is a concept that has permeated the security and policy making realms in recent times. This relationship is examined by using the Baltic nation of Estonia as a model due to the nation being regarded as the ‘most digitally advanced in the world’. The main objective of the thesis is to investigate the relationship between cybersecurity and national resilience and discuss the implications of this relationship in the wider security context. The thesis begins by establishing if a nexus exists between the concept of national resilience and cybersecurity. In order to better understand the potential impact cyber security could have on a nation’s resilience, it is important to establish the relationship between the two concepts. After the nexus is successfully established, the thesis then charts the development of the concept of resilience within the Estonian national security documents. The aim of this exercise is to demonstrate how the concept of resilience has been transformed over the years within an Estonian context while comparing its trajectory to the wider global trend of the concept. The research technique of content analysis is utilised to systematically examine the national security documents of Estonia.

After the concept of resilience is contextualised in case of Estonia, the thesis will endeavor to explore how cybersecurity and national resilience interact on a practical level. The protection of Critical Infrastructure is considered one of the fundamental components of maintaining the resiliency of a nation. In 2018, the fact that National Critical Infrastructure is increasingly reliant on digital systems for operability of its systems was recognised. Thus, cybersecurity plays a key role in protecting these systems from malicious actors in vital sectors such as the energy sector, state agencies, the transport system and the financial sector. This section of the thesis will utilise case studies in the form of the Estonian energy sector and its state agencies to demonstrate the importance of the cybersecurity, i.e. the national resilience nexus.

The final chapter attempts to explain how a healthy civil society tradition can help improve the national resilience building capacities of a nation. This chapter will have a particular focus on the cybersecurity sector as Estonia appears unique in so far as the fact that it possesses volunteer organisations specifically dedicated to defending Estonian cyberspace. This chapter
will draw on Estonia’s long history of inter-agency cooperation to demonstrate how civic responsibility can be utilised to bolster a nation’s resilience. The findings of this research project will be tied together in a concluding section which aims to explain the effect that cybersecurity has on national resilience and what the results from the Estonia case demonstrate in the wider context.
**Introduction**

In the most recent publication of the National Cybersecurity Index, which evaluates the cybersecurity situation of 100 countries all over the world, the small Baltic nation of Estonia ranked third overall, only surpassed by its European neighbours France and Germany respectively.\(^1\) Estonia, one of Europe’s smallest countries reached maximum scores in the following six capacities: cyber threat analysis and information, contribution to global cybersecurity, protection of digital services, protection of personal data, cyber incidents response 24/7, and cyber crisis management.\(^2\) For a country of only 1.3 million people this is an impressive achievement, and is reflective of the fact that Estonia is considered one of the world leaders in digital innovation. It has been lauded as the champion of Europe for online provision of public services in the recent Digital Economy and Society Index produced by the EU, whilst it was also the leading European nation in the Global Cybersecurity Index produced by the International Telecommunication Union.\(^3\) Estonia has become known as the world’s most ‘wired’ country.

Within the literature it is recognised that Estonia’s current superiority in the field of cybersecurity has been partly due to the cyber-attacks that the country experienced in 2007. The nation faced over a month of cyber-attacks which targeted the nation’s critical information infrastructure and has been heralded as the world’s first cyberwar.\(^4\) The events marked a pivotal moment in the field of cybersecurity as it demonstrated to the international community the potential damaging effects cyber operations could have on a state. The attacks coincided with physical riots after a statue commemorating the Soviet liberation of Estonia was moved, sparking riots from the Russian minority. There was a distributed denial of service (DDoS) cyber-attack conducted on the critical infrastructure of the country as government websites were shut down, alongside two major banks and several political parties.\(^5\) The attacks were thought to be politically motivated with an unnamed Estonian official claiming that the attack

---

2 Ibid
“was orchestrated by the Kremlin” despite the fact this has never been officially verified. The attack has since been heralded as a ‘wake-up call’ for Estonia and the wider world as it forced wide scale reforms in the cybersecurity domain resulting in the nation has developing a “world class cybersecurity sector”.7

The importance of effective cybersecurity is becoming increasingly acknowledged by national governments. For example, the UK’s Government Communication Headquarters (GCHQ) recently claimed keeping the UK safe from cyber-attacks is now as important as fighting terrorism.8 This is certainly the case in Estonia or ‘e-Estonia’, the nation named ‘the most advanced digital society in the world’, where citizens file taxes online (95% of Estonians file taxes online), obtain their prescriptions and test results online, sign documents, and vote in general elections online.9 However, what is meant by the use of the term ‘cybersecurity’ can sometimes be ambiguous as the term is often used interchangeably with other terms such as information security, computer security and electronic security. The Estonian Information Authority had to address this problem when creating the Estonian cyber defence strategy as analysis of existing definitions revealed that they did not meet the target criteria of: generalizability, brevity and systematicness.10

Thus, a new definition was developed which would fit the context of Estonian information society and the organisation of security. The working group defined: i) “cybersecurity as: (a) the security of cyber devices and (b) security against threats created through the operation of cyber devices” and

ii) national cybersecurity as: “(a) the security of cyber devices of national importance and (b) protection against threats created through the operation of cyber devices.”11

Furthermore, the working group stressed the centrality of the term cyber device, which is defined as “an information processing device which is able to communicate with all other information...

6 BBC, “How a cyber-attack transformed Estonia”
11 Ibid
processing devices with the ability to communicate”. With such ambiguity regarding the cybersecurity term the above definitions from the Estonian government provide a key insight into how the nation conceptualises cybersecurity. It is of importance for this research project that there is clarity as to the meaning of the key concepts that are central to this research question. The definition provided by the International Telecommunications Union as it offers a broad and comprehensive definition of the concept. This definition as follows:

“Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and 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. The general security objectives comprise the following:

- Availability
- Integrity, which may include authenticity and non-repudiation
- Confidentiality\(^{13}\)

The other key concept that this research project utilises is the concept of national resilience. Resilience, a concept that was originally associated with the ability to bounce back after a disturbance, has now permeated into the field of security and government policy making. Although the genealogic roots of the concept can be traced back to the fields of engineering, psychology and ecology, the concept has increasingly been used as a strategic framework in the security field. Estonia, the subject of this study is one of the countless nations that have subscribed to the superhero-like concept of resilience as it refers heavily in the nation’s last two National Security Concepts. The transition from defensive to more resilient based approaches to security can be understood because of the fact it is geared more toward long term

\(^{12}\) Ibid
\(^{13}\) International Telecommunications Union, “Definition of cybersecurity”, ITU. Available at: https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx (Accessed May 2018)
policy making rather than short term contingency planning. Uncertainties are inherently unpredictable and because resilience presupposes systems with dynamic or multiple equilibria, the concept of resilience emphasises longer-term strategies that reach beyond the existing system state. Within the literature is considered to be the most under researched aspect of the concept of resilience and despite its increasing popularity, a comprehensive definition and understanding of the concept remains allusive. However, it seems that beyond the various definitions there is a tendency to agree that national resilience means society’s sustainability and strength in several diverse realms, including components such as patriotism, optimism, social integration, and trust in political and public institutions.

Despite the apparent importance of both cybersecurity and national resilience to not only Estonia, but numerous Western countries, little academic scholarship has been undertaken documenting the interaction between these two distinct subjects. This thesis aims to address this literature gap by critically analysing the relationship between cybersecurity and its effect on a nation’s resilience, with Estonia used as the chosen case study. Three research sub-questions have been devised in order to successfully complete the goal of this research project, and they are as follows:

1) Does a nexus exist between cybersecurity and national resilience?
2) In what way do the concepts of cybersecurity and resilience interact to increase the national resilience of a nation?
3) With a particular focus on cybersecurity, what role does civil society play in building national resilience in Estonia?

This dissertation has been split up into nine separate chapters with Chapter One comprising of this introduction. Chapter Two deals with the methodological approach that has been adopted for this research project which has focused on qualitative research methods. Chapter Three will

---

15 Ibid.
address the theoretical underpinnings of the study which is based around the Copenhagen School’s securitisation theory.

Chapter Four offers a comprehensive view of the body of literature for this subject matter. The most recent literature on both national resilience and cybersecurity has been analysed in order to give an updated overview of the main themes in the field. Furthermore, a clear literature gap has been identified that justifies the undertaking of this research project.

In Chapter Five, the cybersecurity and national resilience nexus is critically considered. The main premise of this chapter is to determine what impact cybersecurity has on the national resilience of a nation. This chapter demonstrates that a tangible link exists between the two factors and provides the basis for the further discussion of the dissertation topic.

Chapter Six concentrates on tracing the concept of resilience through Estonian security discourse. The chapter is divided into two parts. Part one is dedicated to tracking the development of the concept through the official security documents of the Republic of Estonia. The second part of the chapter deals specifically with the use made of the resilience concept by Estonia, through the analysis of transcripts of a speech given by the Prime Minister of Estonia and, separately, an interview by a well-established expert in the field of cybersecurity. These speech-acts clearly demonstrate the importance now being attributed to the concept of resilience in the context of national security.

Chapter Seven considers particular examples as to the manner in which cybersecurity methods are utilised in order to increase the national resilience of Estonia. There is a key focus on the country’s critical infrastructure as this is arguably the most important pathway through which cybersecurity can bolster Estonia’s national resilience. The analysis concentrates on two sectors of Estonia’s critical infrastructure in this chapter, namely the energy sector and the function of the state agencies of Estonia.

Chapter Eight examines the connection between the strong civil society culture in Estonia and cybersecurity. The existence of civil society is considered by some social scientists as one of the fundamental components of a resilient nation and in the case of Estonia, cybersecurity plays a central role in civil society. This chapter focuses on the Estonian Defence League Cyber Unit.
which is a civil volunteer organisation that aims to protect Estonian cyber-space. Inter-agency cooperation in Estonia is also investigated as it claimed to provide numerous benefits to both parties such as accelerated provision of infrastructure and budgetary benefits.

The final chapter of this thesis will draw together the main findings of this project and discuss how these correspond with the three research questions stated in the introduction. This chapter will also explain the importance of the results in relation to the wider security context and it will also highlight key points for future research.

2. Methodology

2.1 Introduction to Methodology

The research question for this thesis involves the evaluation of the effect that cybersecurity can have on the national resilience of a nation such as Estonia. In order to select the appropriate research methods, it was essential to examine the methodologies of previous studies in the field of resilience. It was discovered that over the broad spectrum of literature that focuses on the concept of national resilience, a variety of methodologies have been used. There are no previous studies that attempt to investigate the effect that cybersecurity has on a state’s national resilience. However, studies have been conducted for which the objective was to measure a particular nation’s resilience, and these have been useful for this research project. Generally, there are two separate approaches to measuring the resilience of a nation which can be categorised by the measurement of resilience building capacities and also the measurement of the manifestation of resilience after a critical event has occurred. This study will adopt a hybrid approach to this issue as it aims to identify how cybersecurity helps to build resilience capacities as well as the role that cybersecurity plays in helping Estonian society withstand a crisis.
2.2 Previous Studies of Resilience

Although research on the measurement of national resilience exist, the scope of these studies is very limited and low in number. This makes it difficult to use past studies as a basis for selecting an appropriate framework for research methods. One of the seminal studies in this field by Daphna Canetti, Israel Wasimel-Manor, Naor Cohen and Carmit Rappaport investigated what the concept of national resilience meant in a democracy and used Israel and the United States as examples. For the purposes of their study, they examined the perceptions of national resilience amongst Israeli and American students employing qualitative research methods.\(^\text{17}\) One of the qualitative methods that the authors utilised was the issuing of questionnaires using open ended questions in order to gauge the respective nation’s perception of national resilience.\(^\text{18}\) This approach was not adopted for this research project as the issuing of questionnaires to Estonian students was considered applicable as a means of determining how cybersecurity impacts national resilience in Estonia. The reason for this action is that this research project does not seek to examine the perceptions of national resilience but is rather more interested in the effect cybersecurity has on the concept.

Daphna Canetti and her colleagues also utilised a content analysis program specifically designed to study textual information called Wordstat, which with its built-in exclusion list removed words with little semantic value and provided the authors with a list of key or unique words.\(^\text{19}\) A similar program called MAXQDA has been employed during content analysis for this thesis. It is a program designed to facilitate and support: qualitative, quantitative and mixed methods research projects. The study by Canetti et al also employed a comparative case study to compare the perception of national resilience in Israel and the United States. Although comparative case studies have their merits, a singular case study has been used for this research project in order to determine the effects of cybersecurity on a state’s national resilience. Estonia provides the perfect model for this investigation for several reasons which will be subsequently explained.


\(^{18}\) Ibid.

\(^{19}\) Ibid
The lack of a clear coherent framework to measure a nation’s societal resilience has limited the development of the concept of national resilience. Academics such as Steiner, Woolvin, and Skerrat have claimed that measuring community resilience remains highly challenging as there is a lack of easily adaptable and practical tools which enable aspects of ‘change’ (or conversely, consistency) to be identified in both qualitative and quantitative ways. Three of the most widely accepted measures of community resilience are: the enhanced critical infrastructure protection program, the DROP model and assessing resilience with mixed qualitative and quantitative techniques (see Figure 1). As the objective of this study is not to measure the resilience of Estonia but rather to investigate the effect that cybersecurity has on the nation’s resilience, mostly qualitative research methods were utilised. This decision was taken because the use of qualitative techniques enables the researcher to capture the richness and complexity of the resilience concept. The following section will detail the quantitative and qualitative techniques that were used during this project.

2.3 Research Methods

Shortly after beginning research for this project, it became apparent that a case study approach to this research question would be appropriate. A case study can be simply defined as an intensive study about a person, a group of people or a unit (such as a country), which is aimed to generalise over several units. When considering the merits of the multiple case study approach, it was initially believed that this would provide the best framework to analyse the issues. The initial research proposal posited that the Baltic States would provide an appropriate comparative study to examine the effect of cybersecurity on the national resilience of small states. However, on reflection, it was decided that a singular case study approach based on one nation would be more effective. The justification for this decision is that a single case study allows the researcher to investigate a particular case in great detail and produces a much deeper and more meaningful understanding of the subject than a multiple case study. Due to the complex and abstract nature of the concept of resilience the multiple case study approach would have required a longer timescale and greater resources in order to produce a study which

effectively demonstrated the effect cybersecurity has on the national resilience of more than one country.

In terms of case selection, Estonia was chosen using the critical case strategy for the selection of samples and cases. A critical case can be defined as having strategic importance in relation to the general problem. A simple generalisation for the critical case could be explained by the quote “If it is valid for this case, it is valid for all (or many cases)” or in its negative form “If it is not valid for this case, then it is not valid for any (or only few) cases.” The question of how to identify a critical case proves much more difficult than simply identifying what constitutes a critical case. No universal methodological principles exist by which one can with certainty identify a critical case. The only general advice that is given states that when looking for a critical case it is a good idea to look for either “most likely” or “least likely” cases, that is, cases likely to either confirm or irrefutably falsify propositions and hypotheses.

The Estonian example fits with the criteria for a critical case on a number of different levels. Perhaps most importantly as was cited in the introduction, Estonia is considered as one of the world leaders in digital innovation. Estonia’s reputation as one of the world’s most ‘wired’ societies makes it a fitting critical case study for this project due to its reliance on cybersecurity for the functioning of the state. The reasoning is that if cybersecurity does not bolster the national resilience of Estonia, then it is most likely that cybersecurity will not bolster the national resilience of any nations of similar size. Finally, in practical terms, the Estonian government release translations of the majority of their official publications which presents the researcher with a viable collection of documents to conduct research.

Basic content analysis of texts is one the most popular research methods for a variety of academic disciplines. It is best known as a methodology for empirically identifying and describing themes or other aspects of communication content, as well as the devices used to deliver this content. Content analysis may address language, content meaning, techniques of communication, specific events, or all these simultaneously. The advantage of using basic content analysis as a research method lies in the ability of a researcher to examine large

---


23 Ibid 231.

amounts of data in a systematic fashion, which helps to identify topics of interest or conversely, it can also be used to determine if content is not present in situations where one may expect it to be. The most basic content analyses use data that are obtained unobtrusively compared to in-person interviews, data are typically within publicly available documents that have been created for reasons other than research. This is a positive as it reduces the reactivity threats to the internal validity of content analyses, as the creators of the data are not likely to shape their work for an unknown audience.

As part of the content analysis process for this thesis the priori generated code approach was utilised because a clear objective already existed which was to identify themes related to resilience in the official security documents of the Estonian Government. This produces a code list or “dictionary” which is used to analyse the collected data. In the case of this research project the terms that were included in the code list were “cybersecurity”, “protection of critical infrastructure”, “civil society”, “resilience (term only)” and “protection of information infrastructure”. In terms of analysis of the data, building an alphabetical concordance list of key terms allows for easy identification of key terms in a text and the context in which they are used. Furthermore, word frequency was used to detail how often specified words were found in the text documents that were studied and demonstrates the omission or infrequent use of an expected term. The analysis of data in basic content analysis usually centres around quantitative analysis as can be seen with the use of word frequency to describe a particular issue or document its importance. As previously mentioned, the software that was used to carry out this content analysis was MAXQDA which allowed for the easy collection, analysis and visualisation of data.

Secondary quantitative sources were extensively utilised during the research process. Data produced by the FM Global Resilience Index, the UN Resilience Chart and the World Economic Forum provided vital data which originated from primary sources. Each of the aforementioned organisations implement a variety of research methods in order to produce unique global resilience indexes. These tools were effective comparative tools as they provided their methodologies and raw data sets for examination. Quantitative data related to the
monitoring of integration in Estonian society from the Institute of Baltic Studies, Estonian Ministry of Culture and Praxis Center for Policy Studies was analysed to provide more of an insight into the attitudes and experiences dominant in Estonian society in integrating people of different nationalities. These sources were vital additions to the research process as they provided sources of primary data which without these studies would have been unavailable.

2.4 Scope and Constraints

One of the biggest constraints while completing the research for this thesis was the researcher’s lack of linguistic skills in Estonian. Although the Estonian Government has released English versions of most of its security documents, some older documents are only accessible in the Estonian language. These documents could have been translated using tools such as Google Translate but due to the unofficial nature of these translations, this was not considered reliable and therefore documents in Estonian were not considered. This represents a clear limitation for this study as the full collection of Estonian security documents could not be considered for analysis. However, after consideration it was felt that the number of official documents published by the Estonian Government in English coupled with the official transcripts of interviews with current and former Estonian officials, provides a sufficient body of material for basic content analysis. Arguably another criticism that could be levelled against this research project in terms of the research methods used is the lack of primary research material. The thesis focused on secondary sources as the majority of the data that was analysed for this project was gathered from official documents from institutions such as the Estonian Government, NATO and the EU.
3. Theoretical Approach

The limitations that are discussed in the above section on methodology as regards the absence of any established framework for the measurement of national resilience, are also of relevance to the question of whether or not there is a theory of security that would form an appropriate framework for the examination of the research question. The limitation regarding the lack of literature in relation to the issue of national resilience in the context of securitisation of the cyber environment, also applies in relation to the dearth of academic study of the key concepts that form the cornerstones of the dissertation topic. It has not been possible to identify a purpose specific theoretical approach from within established theories or frameworks (which have already been developed to analyse and understand different aspects of security), that assists in understanding whether or not the concept of cybersecurity is a security issue that either bolsters or erodes national resilience.

The conclusion that has been reached is that there is no directly applicable theory but that principles of securitisation have a clear relevance. For that reason the theoretical underpinning of the study is based around the Copenhagen School’s securitisation approach.

---

It has a clear and direct relevance to the research and analytical approach that has been taken in this dissertation in examining the new conceptual link between cybersecurity and national resilience. As stated by Mike Bourne in his textbook “Understanding Security”: “While some critical approaches to security have normative intentions in retheorizing security, the Copenhagen School sought the more attenuated goal of developing a new framework for analysis (Buzan et al., 1998). This framework analyses how issues become “security” issues and the implications this has for politics.” This framework facilitates analysis of the process of making something a security issue and this is approached in this dissertation through the basic content analysis and consideration of “speech acts” prior to then considering the evidence that shows how the attempted securitisation of the cyber environment has been accepted by politicians and the Government, security policy makers, and civil society within Estonia as a consequence of the acceptance of the nexus between national resilience and cybersecurity.

The dissertation charts the process of moving the issue of cybersecurity into the realm of national resilience and security politics, having regard to the existential threat to the security of Estonia.

4. Literature Review

The main objective of this literature review is to contextualise the research question for this study. The subject of resilience has been analysed in order to examine the main themes that have emerged from the body of literature. The literature review also aims to highlight key research gaps within the field.

4.1 Genealogy of Resilience

In order to better understand how the concept of resilience has emerged within the field of security studies, it is important to investigate the roots of the concepts. Despite its recent increase in popularity, resilience has been used by academics and practitioners for a number of years. The most basic understanding of resilience can be found through its Latin origin, 29 Ibid, page 52 30 Ibid, see the discussion of speech acts by Bourne at page 53
resiliens “to rebound or recoil.”³¹ One of the earliest documented uses of the term resilience appeared in the field of engineering, related to the resilience of materials. In Thomas Young’s A course of lectures on natural philosophy and the mechanical arts, published in 1807, a short definition was provided, “the resilience of a beam may be considered as proportional to the height from which a given body must fall to break it”.³² The use of the resilience concept within the engineering field can be characterised by its emphasis on the elastic energy that a material can absorb without breaking. Engineers classify a structure as resilient based on its ability to avoid failure. In order for a structure to possess the characteristics associated with resilience, it must include physical strength and robustness, or “the ability of a structure (or part of it) to withstand events (like fire, explosion, impact) or consequences of human errors, without being damaged to an extent disproportionate to the original cause.”³³ The engineering approach to resilience correlates to the robustness concept of the system of resilience used in security studies. Resilience as robustness is the increased ability to absorb perturbations, and accounts for some of the earliest explorations of the concept of resilience and, in particular, its roots in engineering.³⁴

Following the early utilisation of the concept in the field of engineering, it was adopted by academia in the psychology field. When it emerged in the 1970s being defined as a dynamic process creating positive adaptation within the context of significant adversity.³⁵ Authors such as Daniel R. Hanson and Irving I. Gottesman attribute the development of the resilience concept in psychological sciences to Norman Garmezy during this time. His early work focused on the prospective studies of children thought to be at a high risk of Schizophrenia and he became impressed by individuals who experienced hardships but recovered admirably.³⁶ Emmy Warner was one of the first scientists to use the term “resilience” and her pioneering study with her colleague Ruth Smith, shaped the way resilience is perceived today. Their

---

³² Thomas Young, A course of lectures on natural philosophy and the mechanical arts, (London: J Johnson Publishers: 1807) 50.
³⁶ Ibid
ground-breaking longitudinal study of children born into poverty on the Island of Kauai documented the children’s life course with extensive multivariate and longitudinal data that includes biological and psychosocial variables. These studies focused on investigating the resilience concept on communities in order to determine the resilience of individuals to traumatic stresses such as diseases, poverty, hardship and alcohol abuse. Traditionally, academic literature focusing on the subject of resilience in psychology has focused on the individual and the resilient characteristics which they possess. However, since the 1990s, there has been a desire from criminologists, psychologists and social workers to “de-individualise” the concept of resilience and to see it as a social and multifaceted process working at the individual, family, community and societal levels. This provides an insight into how the concept has begun to permeate into national security discourse as the idea of the resilience of a society to adversity has risen in popularity. The use of resilience in psychology has also questioned the assumption that resilience is considered a positive force. Psychological studies which have been conducted in the military context by academics such as Dr Amy Adler, have highlighted that a strong positive emphasis on resilience could potentially send a message stigmatising lack of resilience as a character flaw. This criticism of the concept is reflected in other fields of academic study.

Arguably, the concept of resilience has been most significantly developed in the academic field of ecology within which it is characterised as the ability of an ecosystem to return to a state of equilibrium and maintain its function after a shock or disturbance. In the critical study the Genealogies of Resilience by Jeremy Walker and Melinda Cooper, it is claimed that the concept of resilience was developed within systems ecology in the 1970s as the science of complex adaptive systems. The man who has been credited with developing the resilience concept that is so widely utilised today is Crawford S. Holling. He introduced the concept in his Resilience and Stability of Ecological Systems paper published in 1973 in the following terms: ‘resilience, that is a measure of the persistence of systems and of their ability to absorb change and disturbance and still maintain the same relationship between populations or state

Moreover, Holling’s focus on viewing resilience as the science of complex adaptive systems has played an integral role in the way the concept is used within community and societal resilience today.

Although Holling is regarded by many as the ‘father of the resilience theory’, his work has still been subject to criticism from the academic community. For example, ecologist Richard Klein questions one of Holling’s key assumptions of his original concept of resilience, namely that ecosystems exist in an equilibrium state to which they can return after experiencing a given level of disturbance. Rather he argues that ecosystems are dynamic and evolve continuously in response to external influences taking place over a period of time. Klein’s main argument was that an ecosystem should not be viewed as a static body as it is continually changing and therefore an original equilibrium does not exist and cannot be returned to. Separately, scholars of social science have questioned if Holling’s understanding of resilience can legitimately be harnessed in order to use it effectively in the field of social science. For example, in a study conducted by Olsen, Jerneck, Thoren, Persson and O’Byrne, it is argued that there is a incommensurability between natural and social sciences due to the fact that the resilience vocabulary does not fit with social sciences, whereas core concepts and theories in social science, such as agency, conflict, knowledge and power, are absent from ecological resilience theory.

Despite the criticism of the ecological based concept of resilience and its applicability in social science, most authors on the subject of resilience acknowledge the potential analytical potential of this subject of study. Phillipe Bourbeau, one of the biggest proponents of the use of resilience in the social sciences, effectively summarises the view that should be taken by social scientists on the ecological roots of resilience. He states that “accepting that the ecological definition of

44 Ibid
resilience is but one possible facet of a broader, multidimensional concept offers a richer approach”. Bourbeau’s statement is correct as the diverse roots of the concept of resilience has made it more flexible but, on the other hand, the diversity has played a role in the possible ambiguity of the concept.

4.2 National Resilience and Security

In 2005, K.U. Menon, the former head of the National Resilience Division in Singapore claimed that national resilience is perhaps the least researched aspect in the whole subject of resilience. Thirteen years later and scholars such as Hamilton Bean believe that the subject of national resilience is under researched. Bean asserts that the research on the concept of national resilience has not kept pace with its growing invocation within national preparedness strategy and discourse. Building on Bean’s argument, despite the concept’s current popularity with national policy makers and governments, its true definition and value remains ambiguous for practitioners and academics alike. As previously mentioned, the diverse background and genealogical roots of the concept from the fields of engineering, psychology and ecology could explain this ambiguity. This has resulted in a multitude of definitions which has meant that the conceptual framework of resilience is very difficult to utilise as there lacks a uniformed understanding of the concept. Resilience has become an important component of the national security documents for a number of Western countries such as the United States, Canada, the Netherlands, Australia, France, the UK and Estonia. This approach to security and disaster management is not only favoured by national governments as some of the world’s largest non-governmental organisations have utilised resilience over the last decade. NATO for example, defines the concept as “resilience is a society’s ability to resist and recover easily and quickly from these shocks, combining civilian, economic, commercial and military factors. In sum, resilience is the combination of civil preparedness and military capacity”. Despite the ambiguity of the exact definition of national resilience, the term has been adopted by some of

46 Bourbeau, “A genealogy of resilience” 12.
49 NATO, “Resilience and Article 3”, NATO, June 2016. Available at: https://www.nato.int/cps/ic/natoig/topics_132722.htm (Accessed May 2018)
the world’s most militarily powerful nations and organisations demonstrating the increasing importance of the concept in the field of security.

The roots of national resilience in the context of national security can be traced back to the tragic events that shook New York and the wider world on the 11th September 2001. This event demonstrated the potential catastrophic psychological and damaging effects that non-state actors could have on one of the most powerful nations in the world. It highlighted the shift from traditional armed conflicts between states to the rise of non-state actors as sources of threats such as terrorist groups, transnational crime and insurgent groups. This resulted in a clear desire for a new approach to security that improved the preparedness of societies and enabled governments to manage the expanding myriad of new threats that were emerging in the world. It has been argued that “risk and “resilience” have begun to constitute a conceptual pair similar to “threat” and “defence”.50

The traditional approach to security which focuses on the nexus between “threat” and “defence” has become increasingly inadequate in dealing with security issues that are progressively becoming more diverse and dangerous that require non-military solutions. As Olaf Corry correctly explains, “it makes little sense to ‘defend’ against catastrophic climate change, pandemics, economic meltdowns, or even certain kinds of terrorism, insofar as security concerns such as these are based primarily on uncertainty, are located in the future, and often lack clear adversaries”.51 In Mike Bourne’s book Understanding Security, he offers a concise definition of national resilience from a security perspective as he describes it as “the ability to minimise the damage of an earthquake or terrorist attack and to ensure minimal disruption of daily life, rather than merely security as protection, which prevents the event in the first place”.52 Although there are countless other definitions of national resilience which offer a broader view of the concept, this definition highlights the nexus between resilience and risk. One of the fundamental components of the concept of resilience in the security field is that resilience seeks to minimise the damage that is caused by a particular event after it has occurred, rather than attempting to eradicate the threat altogether. This approach from security differs from the traditional view of security where the ultimate condition of security which is to exist in a state without threats to life or something valued. The resilience approaches accept

50 Corry, “From Defense to Resilience” 256.
51 Corry, “From Defense to Resilience”, 257.
a degree of uncertainty, but also are founded on the premise that risks can be classified, quantified and predicted to some degree.\textsuperscript{53}

Resilience has been depicted by sections of the academic community as an all-conquering, 'superhero' type concept that can be turned to any problem, security or otherwise. However, this is not realistic as resilience should not be viewed as a quality, paradigm or theory to resolve the world’s most pressing geo-political and security issues.\textsuperscript{54} Due to the complex background to the concept of resilience, it is almost inconceivable that a comprehensive theory of resilience can be developed that has a wide application across a range of academic fields. Instead, it is more useful from an academic perspective to view resilience as more of an abstract concept, metaphor or lens to view issues through. Jon Coaffee believes that resilience should be viewed as a metaphor which can be applied in a variety of national and international contexts—a translation term which allows connections to be made between different strands of research and common terminology and consistent threads of analysis.\textsuperscript{55} Thus, there are several dimensions in which the concept of resilience can be articulated, which offers an alternative to traditional approaches of security which are no longer suitable in today’s security environment.\textsuperscript{56}

Despite the clear potential in the field of international relations for the use of the concept, it has received stringent criticisms from some parts of the academic community. Even the biggest advocates of resilience acknowledge that more work has to be done to better theorize the relationship the concept and international relations and security related issues. One of the most common criticisms mounted against the operational use of national or societal resilience is related to the process of the prioritisation of resources. If the strategic objective of a country is to make the nation more resilient, resource prioritisation is an unfortunate reality of this strategy. As an example, a situation may arise where there is a decision to prioritise the resilience of the electric supply to a densely populated area where there is an abundance of critical infrastructure, in preference to the supply to a more remote area with a sparse

\textsuperscript{53} Bourne, Understanding Security, 110.
\textsuperscript{56} Coaffee,"From Counterterrorism to Resilience." 399.
population and limited industrial production. The provision of security is supposed to be available to all who live within a society and if anything was to occur which endangered the population of areas neglected due to resource prioritisation, questions must be asked regarding the state’s ability to provide security to its citizens. Jon Coaffee argues that it is not only geographical areas and commercial industries that can be affected by resource prioritisation due to a resilient based strategy. He warns that despite the potential for terrorism to inflict massive damage, there are serious risks that governments should not de-prioritise other events, such as natural disasters, health pandemics and weather abnormalities. States face a difficult challenge to successfully balance uncertainty with security without leaving sections of society vulnerable to possible harm.

4.3 Theoretical Underpinning of Resilience.

In terms of security studies, most of the literature that has focused on the theoretical underpinnings of the concept of resilience can be described as homogenous. The theory has focused on resilience based on neo-liberal governance. As a security concept, resilience has been understood through the prism of Foucault’s later work on governmentality. Jonathan Joseph, one the most outspoken critics of the concept of resilience in the field of international relations believes that it is not only a shallow concept that is nothing more than a ‘buzzword’ but should be understood in the context of rolling out neo-liberal governmentality. Neo-liberal governmentality can be best defined as through processes of neo-liberalism, the State has “hollowed out” some of its cartographic responsibilities and delegated power to individuals who are at a lower geographical scale. Joseph argues that resilience has an inherently neo-liberal ontology which places more emphasis on individual responsibility, adaptability and preparedness. Joseph’s argument is based on the idea that resilient strategies allow the state to abdicate responsibility in crises as an individual must take responsibility for their own security. This corresponds with the notion that the development of national resilience has led to the idea of the ‘responsible citizen’ in accordance with new techniques of governmentality.

---

58 Coaffee, "From Counterterrorism to Resilience." 399.
61 Josesph, “Resilience as embedded neo-liberalism”, 40.
the replacement of state-centric ‘protective’ security approaches with those emphasising ‘self-organising’ human security.\textsuperscript{62} The main premise of the criticism that Joseph and other authors propose against resilience, is that beneath resilience there is a dehumanising political agenda, the continuity of a state’s dominance and a strategy for creating unequal regimes of power.\textsuperscript{63}

However, Philippe Bourbeau refutes the argument that the broad concept of resilience in international relations should be regarded as simply a vehicle for neo-liberal governance. He claims critics have made the mistake of equating one government’s particular use of resilience as a neo-liberal device for governance as a representation of the concept as a whole.\textsuperscript{64} This refers to Jonathan Joseph’s claims that the US and UK security documents related to resilience demonstrate the governmentality approach of operating from a distance through the ‘responsibilising’ of various actors.\textsuperscript{65} The argument throughout this thesis agrees with Bourbeau that Joseph’s claims are too much of a generalisation of the concept of resilience as a whole. Furthermore, Olaf Corry goes one step further in his defence of resilience as he claims that resilience potentially contradicts the tenets of neo-liberalism, emphasising the inherent links between social and ecological systems, the necessity for collective rather than individual level rationality to safeguard non-economic system limits, the role of self-reflection, self-critique and adaptive learning, and the need to build redundancy and diversity into socio-ecological systems.\textsuperscript{66} The study of the resilience concept in the field of security would benefit from a more heterogenous body of literature in relation to the theoretical underpinnings of the concept of resilience. More research must be done to investigate how the concept of resilience interacts with established theories of international relations.

4.4 Resilience and Estonia

In the academic sphere, there is a distinct lack of literature focusing on the concept of national or societal resilience and how it is applied in Estonia. Academics such as Jon Coaffee, Keiran Hardy and Jonathan Joseph have produced extensive work on the UK’s approach to resilience and have studied the concept in great detail. In terms of literature on US resilience strategies


\textsuperscript{63} Bourbeau, "Resilience and International Politics", 376.

\textsuperscript{64} Bourbeau, "Resilience and International Politics", 382.

\textsuperscript{65} Josesph, "Resilience as embedded neo-liberalism", 48.

\textsuperscript{66} Corry, "From Defense to Resilience", 271.
associated with the US Homeland Security approach, there is an abundance with academics such as Philip Palin, Jerome H. Kahan and Karen L. Petersen contributing to the subject. However, the same cannot be said for Estonia as there is a limited amount of literature available. Two scholars who have studied Estonia’s relationship with resilience are Tomas Jermalivicius and Merle Parmak. The main premise of their article was that the promotion of societal resilience in Estonia was a better approach to security than psychological defence.\textsuperscript{67} The duo claim that resilience as a holistic concept is far better suited as a framework for thinking about how to ensure the flexibility and the adaption of a small nation that wants to survive and prosper in a turbulent security environment without the risk of developing a siege mentality or drawing charges of manipulation that ‘psychological defence’ is susceptible to.\textsuperscript{68} This is an important point in regards to this thesis as resilience is an appropriate strategy for a small country like Estonia that does not possess the resources to implement a complete defence strategy and must prioritise, something that is inescapable with a resilience based strategy. Parmak has also produced other work that documents the concept of national resilience in a multinational society which is applicable to Estonia due to its sizeable ethnic Russian population. Her article rightly highlights that excluded or unintegrated sub-communities may prove to be very resilient in themselves but not for the nation, thus in fact posing an additional threat to political stability during the time of crisis.\textsuperscript{69}

In summary, there is a substantial literature gap in the field of national resilience in Estonia. Not only is the academic research on Estonian national resilience limited, the subject of national resilience is the least researched area of the whole resilience concept. This literature review has charted the genealogy of the concept of resilience as the diverse roots of the concept provide an effective insight into how the concept’s flexible nature has developed in recent times. The concept of resilience was adopted in the field of security studies and international relations as a new approach to traditional security theories and methods. Scholars believe the concept’s flexibility and diverse background makes it an appropriate concept to apply to security matters and national policy making in the security sphere. This originates from the belief that the current security environment contains a myriad of new threats that are always evolving, and a new concept was required to better deal with these dangers. Despite the


\textsuperscript{68} Jermalivicius and Parmak, “Towards a resilient society”, 16.

\textsuperscript{69} Parmak, “National Resilience in Multinational Societies” 118.
concept’s diverse background, the theoretical approach to the concept of resilience in the field of international relations has been dominated by one school of thought. Scholars have used Foucault’s concept of ‘governmentality’ to criticise the concept of resilience and highlight its apparent negative characteristics. However, the concept of resilience possesses significant potential as a concept in this field and this thesis aims to add to the limited literature on the concept of national resilience and in particular, Estonian national resilience. The next section of the literature review will briefly outline the key arguments associated with cybersecurity and its nexus with national resilience.

4.5 Cybersecurity

The majority of this literature review has focused on the concept of resilience and in particular national resilience as this is the main theme of this thesis. Cybersecurity can be viewed as the variable in this project as it aims to identify the role that cybersecurity has on the concept of national resilience. Thus, the main themes in cybersecurity literature will be identified in a briefer fashion than the previous section.

Cybersecurity was first used by computer scientists in the early 1990s to underline a series of insecurities related to networked computers, but it moved beyond a mere technical conception of computer security when proponents urged that threats arising from digital technologies could have devastating societal effects. Cybersecurity has developed into one of the most fundamental components of national security in recent years. Releasing its second Global Cybersecurity Index, the International Telecommunications Union said about 38% of countries have a published cybersecurity strategy and an additional 12% of governments are in the process of developing one. In most literature, cybersecurity has been used as an umbrella term as it has been utilised for a variety of topics related to information security. The referent object of security in relation to cybersecurity has become a contentious issue. Information and communication technology (ICT), which has been used interchangeably with cybersecurity, deals with the protection of the actual technology-based systems on which information is


commonly stored and/or transmitted. Furthermore, information security extends this definition of the assets to be protected to include all aspects of the information itself. It thus includes the protection of the underlying ICT assets, and then goes beyond just the technology to include information that is not stored or communicated directly using ICT. Thus, cybersecurity should be seen as an expansion of information security as cyber should be about protecting more than just the information, information resources, of a person/organisation but rather is about the protection of the person(s) using resources in a cyber environment and about the protection of any other assets, including those belonging to society in general, that have been exposed to risk as a result of vulnerabilities stemming from the use of ICT (see Figure 2 for graphic depiction). This has led to some constructivists to argue that cybersecurity has become a new sector of security, in which two referent objects of security, the network and the individual are interlinked. This not only securitises cyber infrastructure but also shifts security from the political to the technical, since cybersecurity practices are entwined with the technical knowledge of experts in the private sector and the development of new technologies.

4.6 Cybersecurity and Theory

The discussion in the paragraph above acts as a useful link to introduce one of the most important themes in cybersecurity literature at the current time. The Copenhagen School argues that security is a speech act that securitises, i.e. that it constitutes one or more referent objects, historically the nation or the state, as threatened in respect of their physical or ideational survival and therefore in urgent need of protection. In terms of cybersecurity the Copenhagen School has dealt with the subject as an example of an attempted securitisation. However, in 2018 cybersecurity is successfully securitised as evidenced by such institutional developments as the establishment of the Commission on Critical Infrastructure Protection by President Clinton in 1996, the prominent location of cybersecurity within the Department of Homeland Security, President Bush’s formulation of The National Strategy to Secure Cyberspace in 2003,

---

73 Ibid 100.
74 Ibid 101.
75 Bourne, Understanding Security, 91.
76 Ibid.
and the creation of a NATO-backed cyber defence centre in Estonia in 2008.\textsuperscript{78} Lene Hansen and Helen Nissenbaum have significantly advanced the literature on the securitisation of cybersecurity as they theorise that cybersecurity should be considered as a distinct sector with a particular constellation of threats and referent objects. They utilised the 2007 Estonia cyber-attacks to illustrate their theoretical framework. As the riots spread from the streets to the Internet, Estonian authorities’ cyber securitisation articulated attacks on the network as threats to Estonian political sovereignty as well as to cultural and national identity.\textsuperscript{79} The ability of Estonian securitising actors to have the attacks accepted as “the first war in cyberspace”, and to have them prominently covered by the world press, makes for at least a partially successful case of cyber securitisation.\textsuperscript{80} Although the Estonian case cannot be considered a completely successful case framing the cyber-attack in a securitised manner, the nation’s hypersecuritisation of certain events did bring some success in convincing the international community that this situation should be considered as an act of war.

However, there are authors such as Clement Guitton who have claimed that nations who have securitised the issue of cybersecurity by including the concept in their national security strategies have done so without possessing the sufficient grounds.\textsuperscript{81} This builds upon the argument that an over-securitisation tendency or an over exaggeration of the power of cyber threats, exist because of the application of traditional military thinking to something completely unique (cyber space).\textsuperscript{82} Scholars such as Nikola Schmidt who hold this view, base their argument around the assumption that cyber-attacks do not have the ability to seriously impact a nation’s critical infrastructure and pose a threat to human life.\textsuperscript{83} However, this is certainly not the case as actors with malicious intentions have demonstrated their willingness, and also their capabilities, to target national critical infrastructure with the attacks on Ukraine in 2015 as a clear example. This is the main factor as to why this thesis follows the line of thinking that cybersecurity should rightfully be securitised by nations as it cannot be argued that cyber-attacks do not pose a real threat to society.

\textsuperscript{78} Hansen and Nissenbaum, “Digital Disaster”, 1157.
\textsuperscript{79} Ibid 1169.
\textsuperscript{80} Ibid
\textsuperscript{81} Clement Guitton. “Cyber Insecurity as a National Threat: Overreaction from Germany, France and the UK?” \textit{European Security} 22, no. 1 (2013): 32.
\textsuperscript{83} Ibid 33.
There have been extensive discussions regarding how established international relations theory can be applied to an emerging cybersecurity field. At the current time, there lacks a clear consensus about how theoretical frameworks interact with cybersecurity topics. This relates to the trend that there is currently a revolution in military affairs in which technological advances have a dramatic impact on the character and contrast of combat operations. In the cyber context, this forms the undertones of Kello’s work that suggests that the future of cyber war will forever change the way states interact with each other. It has been speculated by sections of the academic community that the emergence of cybersecurity and its growing importance to national security has the potential to add to the power and capacity of small states.

Estonia appears to prove this theory as it holds disproportionate cyber power because of its experience after the 2007 cyber-attacks and is now a major centre for cyber defence for the NATO Alliance. Estonia is home to the NATO Cooperative Cyber Defence Centre of Excellence which is a multinational and interdisciplinary hub of cyber defence expertise. It is a recognised norm setter in relation to cybersecurity issues in the international stage and it is home to “the world’s largest and most advanced international technical live-fire cyber defence exercise’- the Locked Shields event. After the 2007 cyber-attacks on Estonia, it came to be regarded as a leader in cybersecurity and the country used this to its advantage in the promotion of self-entrepreneurial experts as a critical resource to be tapped in neo-liberal Estonia. It could be argued that this provides empirical evidence that the emergence of cybersecurity has given increased power and capacity to smaller states. However, Estonia appears to be a unique case as the balance of power remains with the well-established powers of the world and cyber technologies will only reinforce this.

Cyber weapons are not simple and cheap weapons to leverage, they are complicated, expensive and difficult to utilise for offensive and defensive intent. While the field of cybersecurity is

---

85 Valeriano and Maness, “International Relations Theory and Cybersecurity”, 261
87 Valeriano and Maness, “International Relations Theory and Cybersecurity”, 261
not new, the intellectual maturity is developing.\textsuperscript{88} Much of the work to be done in the future requires greater consideration of methods, empirics, and evidence, as well as critical epistemological approaches that would challenge the nature of the institutional arrangements concerning cyber questions.\textsuperscript{89} Similarly to the national resilience field, the topic of cybersecurity is an ever-growing body of literature that holds the potential for both traditional and innovative international relations theorists to interact with the concept. In terms of cybersecurity literature related to Estonia, the majority of it has been dedicated to the 2007 cyber-attacks on the nation. Many have used the attacks as case studies to investigate a potential hypothesis or discuss the implications of the attacks on the cybersecurity field. However, there has been a complete lack of academic scholarship dedicated to the nation’s dependence on cybersecurity and the effect this has on Estonia’s national resilience. This thesis aims to address this literature gap and investigate the ways in which cybersecurity interacts with the popular concept of national resilience by using Estonian as a case study.

To conclude this chapter, this literature review has endeavoured to examine some of the key themes which exist within the literature on national resilience and cybersecurity. The main objective of this chapter was to contextualise the research question of this thesis. A clear literature gap has been identified as currently there are no studies which focus on the potential effect that cybersecurity can have on a nation’s resilience. Furthermore, for a country that relies so heavily on cybersecurity for the functioning of the state, it is surprising that no previous studies exist documenting the impact cybersecurity has on the national resilience of Estonia.

\textsuperscript{88} Ibid 269.
\textsuperscript{89} Ibid
5. Establishing the nexus between cybersecurity and national resilience

This chapter aims to answer the following question: what if any, impact does cybersecurity play in a nation’s resilience building capacities. The question will utilise the community
resilience framework by Norris et al to investigate the role that cybersecurity plays in the building and maintaining of national resilience in Estonia.

5.1 The Cybersecurity and National Resilience Nexus

Before investigating the effect that cybersecurity has on the national resilience of Estonia, it is necessary to determine the nature of the inter-relationship in general terms. As previously mentioned, limited research exists which documents the relationship between cybersecurity and national resilience. As no coherent framework presently exists which identifies the fundamental capacities of national resilience, this thesis will borrow ideas developed in the field of community resilience. The framework that will be utilised was developed by Fran H. Norris, Susan P. Stevens, Betty Pfefferbaum, Karen F. Wyche and Rose L. Pfefferbaum. In their framework, resilience emerges from a set of adaptive capacities and thus, community resilience is established through a set of networked adaptive capacities. For Norris et al. resilience depends on both the resources themselves and the dynamic attributes of those resources (i.e. robustness, redundancy, rapidity); they use the term “adaptive capacities” to capture this combination. Their framework emphasises the importance of the adaptability aspect of resilience as they claim that capacities become adaptive capacities when they are robust, redundant or rapidly accessible and thus able to offset a new stressor, danger or surprise. The networked adaptive capacities that the authors have developed are as follows: Economic Development, Social Capital, Information and Communication and Community Competence (See Figure 3).

This chapter will focus on the “Information and Communication” node of the above diagram. Norris et al argue that information and communication become vital in emergencies as people need accurate information about the danger and behavioural options, and they need it quickly. This refers to the availability and performance of the communication infrastructure of a nation.

---


91 Ibid 136.
92 Ibid, 136.
93 Ibid 140.
during a crisis as it must be available at all times to effectively delivery accurate information to its citizens. The importance of cybersecurity in this field should not be underestimated due to the fact that a growing number of people consume their news and information through online sources.

NATO has reiterated the importance of information and communication systems as it has provided seven baseline requirements for national resilience that the Allies can use to measure themselves against. Two of the seven baseline requirements are related to information and communication. The first baseline requirement is “the assured continuity of government and critical government service: for instance, the ability to make decisions, communicate them and enforce them in a crisis”. The sixth baseline requirement reiterates the need for: “Resilient civil communication systems: ensuring that telecoms and cybernetworks function even under crisis conditions with sufficient back up capacity”.94 Further, NATO’s Deputy Assistant Secretary General for Emerging Security Challenges and regular lecturer Jamie Shea has claimed that cyber space is the perhaps the most extreme vulnerability to a nation’s resilience.95 He has stated that as we move from the internet of things to the internet of everything, more and more of the infrastructure that we depend on for the normal functioning of our lives is being automated or controlled from remoter distances or integrated into ever more complex networks.96

Actual evidence of the aforementioned threats to the information and communication systems is provided by the events that took place in Estonia in 2007. As this dissertation has already briefly touched upon, Estonia was the victim of the first ever cyberwar incident when it was attacked in the Spring of 2007. Multiple botnets were used to launch a Distributed Denial of Service Attack (DDoS), which is similar to Denial of Service Attack (DoS) in that a network is flooded with as many requests as possible such that the network becomes so slow it is effectively unable to respond to legitimate requests. However, in the case of a DDoS attack, instead of one system launching the requests, thousands of compromised systems flood a networks bandwidth making it crash under the enormous load or become so slow it is the

94 NATO, “Resilience and Article 3”, NATO, June 22nd, 2016, Available at: https://www.nato.int/cps/su/natohq/topics_132722.htm (Accessed March 2018)
96 Ibid.
equivalent to being unavailable or offline.\textsuperscript{97} These attacks targeted the Estonian Parliament, Estonian Ministries, banks, newspaper and broadcasters. Their websites were unavailable to Estonian citizens and left them unable to keep up to date with what was happening in the country. Fortunately, the consequences of the attacks were limited and were resolved through international co-operation. By blocking internet traffic from outside Estonia, the websites were made operational again. Although the effects of the attacks could have been much worse, they served as a wake-up call to the potential dangers of cyber-attacks. Imagine a scenario where these DDoS attacks were launched alongside other forms of hybrid warfare by an aggressor to cause chaos and instability in Estonia. If the government pages and news broadcaster websites were offline, the government could fail in its obligation to inform the population that the country was under attack. This scenario highlights the importance of cybersecurity to a nation’s resilience as it plays a key role in maintaining the operational channels of a country’s information and communication infrastructure and ensuring trusted sources of information are being released to a nation’s citizens.

It is not only large international inter-governmental organisations such as NATO that have acknowledged the impact of cybersecurity on a nation’s resilience. FM Global, is a mutual insurance company with capital, scientific research capability and engineering expertise that are solely dedicated to property risk management and “protecting the resilience of its clients-owners”.\textsuperscript{98} The company provides services to one-third of Fortune 1000 companies to mitigate risks in the business market. It has created a Global Resilience Index with twelve drivers of operational resilience which are grouped into three categories: economic, supply chain and risk quality.\textsuperscript{99} These combine to form the composite index with scores bound on a scale of 0 to 100, with 0 representing the lowest resilience and 100 being the highest resilience. The methodology for the 2018 Global Resilience Index states that cyber risk has become an increasingly important driver of resilience and is now classed as one of the twelve drivers of operational resilience under the risk quality category. FM Global defines this driver as inherent cyber risk which combines a country’s vulnerability to cyber-attack with the country’s ability to recover


In the most recent 2018 Global Resilience Index Estonia scored a 74.7 out of 100 and ranked 29th out of 130 countries included in the index. Furthermore, in the risk quality category which takes into account the inherent cyber risk of a country, Estonia ranked 28 out of 130. The recent inclusion of cybersecurity as an operational driver of resilience is very telling as it demonstrates the value that multi-national companies such as FM Global who work with resilience are now placing on the concept.

In the World Economic Forum’s most recent Global Risks Report 2018, 13th edition, similar claims about the importance of cybersecurity are made. The report highlights that cybersecurity risks are always growing both in their prevalence and their disruptive potential. The executive summary of the report also states that “another growing trend is the use of cyber-attacks to target critical infrastructure and strategic industrial sectors raising fears that, in a worst-case scenario, attackers could trigger a breakdown in the systems that keep societies functioning”.

This is an important point to emphasise because in the 21st century this is perhaps cybersecurity’s most critical role in the context of a nation’s resilience. The increasing integration of a nation’s physical infrastructure into the virtual world has increased the dependence on the cyber sector to ensure the maintenance of essential services and infrastructure.

The Global Risks Interconnections Map 2018 (represented as Figure 4) effectively portrays the interconnectability of the global risks that the world is currently facing. In particular it is worth noting the interconnectivity of cyber-attacks with both failure of critical infrastructure and the critical information infrastructure breakdown nodes. The width of the lines connecting the nodes illustrates the strength of relationship between each risk and from the Risk Interconnection Map it is clear that there is a strong correlation between potential cyber-attacks and the failure of critical infrastructure and the breakdown of critical information infrastructure. This is something which has been recognised by the Estonian Government for over a decade. In its first ever cyber-security strategy published in 2008, the need for cyber-

---

102 FM Global, “FM Global Resilience Index: Estonia”, 2018,
security to bolster requirements for the security of critical infrastructure in order to increase its resistance and that of related services, against threats in cyberspace was recognised.\textsuperscript{104}

It is useful to make reference to the Rockefeller Institute definition of resilience which is in the following terms:

“The capacity of individuals, communities and systems to survive, adapt, and grow in the face of stress and shocks, and even transform when conditions require it. Building resilience is about making people, communities and systems better prepared to withstand catastrophic events—both natural and manmade—and able to bounce back more quickly and emerge stronger from these shocks and stresses.\textsuperscript{105}"

From this definition it is clear that maintaining the operational state of critical infrastructure and their connected systems is a key factor in ensuring that a nation is able to withstand catastrophic events, both natural and manmade. The overall resilience of modern societies is largely determined by, and dependent on the resilience of their critical infrastructures such as energy grids, transportation systems, governmental bodies and water supply.\textsuperscript{106} As information technology continues to develop it provides more and more possibilities to make critical infrastructures “smarter”, while also creating more risks and vulnerabilities. Thus, the importance of cybersecurity to the protection of critical infrastructure systems of a nation is greater than ever. In summary, this chapter demonstrated that there is a tangible link between cybersecurity and the building and preservation of a nation’s resilience. As NATO has highlighted, the assured continuity of government and critical government services, resilient energy supplies, resilient civil communications systems and resilient transport systems are all fundamental requirements for a nation’s resilience. The prominent role of cybersecurity in each of these components of a nation’s critical infrastructure demonstrates the nexus between the concepts of cybersecurity and national resilience.


MSc SECINTEL Independent Study (Dissertation)

(Figure 3)
Survey respondents were asked to identify between three and six pairs of global risks they believe to be most interconnected (Figure 4).

6. Tracing the Concept of Resilience Through Estonian Security Discourse

This chapter will aim to chart the development of the resilience concept through the official security documents of the Estonian Government. The purpose of this exercise is to demonstrate the increased importance of the concept to Estonian security policy makers. This task will also help to provide an insight into how the concept has been conceptualised in the Estonian security discourse.

6.1 Brief Introduction of Research Design.

The list of official documents that were analysed during the content analysis process can be viewed in the results table (see Figure 5). This list is not all encompassing as some older security documents were not available from online sources or were only available in the Estonian language. However, of significance is the fact that the research for this project utilised all the documents that were relevant and available to this research question. The documents analysed provide an adequate sample of official documentary evidence to effectively demonstrate growing popularity of the concept within Estonian security discourse. Before discussing the results of the analysis, it is first necessary to define the “codes” which were used during the content analysis process. The “code list” or “dictionary” was created beforehand utilising some of the main themes which have been attributed to a resilient society, mainly; “cybersecurity”, “protection of critical infrastructure”, “civil society”, “resilience (term only)” and “protection of information infrastructure”. Each text was examined thoroughly and samples of the text that referred to the aforementioned code themes were coded accordingly. As an example, in the 2011 Estonian Defence Strategy, under the heading of the development priorities of the Rescue Board in the field of national defence the text states that one of the priorities is as follows: “c) Developing an explosives removal capability that is aimed at clearing critical civil infrastructure from unexploded ordnance and thereby preventing mass casualties that may result in such eventualities”.108 This sample of text was coded using the “protection of critical infrastructure” code due to the content of the passage. The remaining

---

passages of text in the 2011 National Defence Strategy alongside the remaining documents that were examined during this research process were research using this analytical framework.

The only exception that must be highlighted is related to the “resilience (term only)” code, as the name suggests, it was only instances where the literal term itself appeared in the text that constituted the use of this particular code. This was due to the importance of the “resilience” term as the objective was to identify the concept in its own right in the official Estonian documentation. This differs from the rest of the code list as they were used to code any sections of text that were interpreted to be describing themes which directly related to the “protection of critical infrastructure”, “civil society”, “cybersecurity” and “protection of information of infrastructure”.

6.2 Analysis of Results

The first objective of the content analysis research design was to chronologically track the resilience term through the Estonian national security documents. This task was undertaken as it demonstrated the timeline of the term’s use in an Estonian context and could then be compared against the international trend. In the 2004 National Security Concept of Estonia the term “resilience” was not used once in the document (see Figure 5). The purpose of the document was to present the goals and guidance of Estonia’s National Security Policy and a general evaluation of the existing security environment.109 The document has a medium-term perspective and replaces the 2001 security policy document which focused on Estonia’s accession to NATO and the EU.110 As the results in the table demonstrates, there were very limited references to any of the predetermined codes used for this research. Interestingly, although there were two samples in text that warranted the use of the “cybersecurity” code, the term itself was not present in the text. The absence of the words resilience and cybersecurity in this document is very telling. Academic and practical discussions of cybersecurity were still largely theoretical in 2004 as the world was yet to experience its first instance of cyberwar and appreciate the potentially devastating risks within cyberspace. Furthermore, the absence of the resilience term can be explained by the relative infancy of the term within the context of

110 Ibid.
security in 2004. As previously mentioned in the literature review, the concept of resilience within the security context can trace its roots back to the aftermath of the 9/11 attacks in New York in 2001. With practitioners and academics alike attempting to find a better approach to security to deal with new emerging security threats, the concept of resilience began to appear within security discourse. However, resilience was not the ubiquitous term that we see used today in numerous Western nation’s security strategies.

The first security document produced by the Estonian Government within which the concept of resilience is directly mentioned is the 2008-2013 Estonian Cybersecurity Strategy. This document was created in the wake of the infamous 2007 cyber-attacks which targeted Estonia. The document was created as the Estonian Government acknowledged that “the recurrence and growing incidence of cyber-attacks indicate the start of a new era in which the security of cyberspace acquires a global dimension and the protection of critical information systems must be elevated, in terms of national security, on a par with traditional defence interests”. The short time frame between the 2007 cyber-attacks and the creation of this document offers an explanation for the exponentially high level of the “cybersecurity” code occurring in this document. The attacks were part of the reason why the document was drafted in the first place and this is clearly demonstrated within the text. Although the focus of this document was almost solely on “cybersecurity”, “resilience” was mentioned on one occasion in the text. The use of the term was the necessity of the seamless operability of the information infrastructure of Estonia which supports critical infrastructure and on its resilience against attack. The introduction of the term in the 2008 document coincides with the increasing popularity of the concept in the security domain as academics such as Jon Coaffee began to develop the concept within the urban security field.

As Table 1 demonstrates, it was not until the 2010 National Security Concept of Estonia that the concept of resilience began to establish itself more widely within Estonian security

---


112 Ibid 13.

discourse. For the first time, the concept of resilience was given a whole chapter within an official Estonian security document. This is a marked change from two years prior when the concept was merely mentioned once. Estonia were not the only Western country to release a new version of their National Security Concept in 2010. Other nations such as the United Kingdom, United States, New Zealand and the Netherlands released documents describing the uncertain age that we currently live with its myriad of risks. Apart from the commonality of the release date of the documents, Estonia’s 2010 National Security concept shared other similarities with these nations. Significantly, there was a substantial use of the ‘resilience’ term throughout the security documents of the aforementioned countries. 2010 marked the time period where resilience began to permeate into the security strategies of a number of countries and became the ‘buzzword’ that we know today. Estonia embraced the increasingly popular term along with large swathes of the security as they looked for a broad security concept which entailed the involvement of all sectors of society. The nexus with cybersecurity was recognised by the Estonian Government as early as 2010 as the National Security Concept states that ‘The dependence of countries’ resilience on the use of cyberspace is growing’.

One of the main benefits of utilising content analysis is that it not only highlights when a theme or term is recurring within a document but can also highlight its omittance. The 2011 National Defence Strategy serves as an example of this as Table 1 pinpoints the fact that “resilience” was only coded once while completing analysis of this particular document. This is somewhat surprising as the document itself states that “The 2011 National Defence Strategy is based on the National Security Concept of Estonia, which was endorsed by the Riigikogu in 2010”, which would lead one to expect the concept of resilience to play a more prominent role given its weight in the 2010 document. One can only speculate regarding this irregularity, but the answer could lie within the separate purposes of these documents. The National Security Concept constitutes a framework document, forming the basis for the preparation of specific development and action plan, whereas the main goal of the National Defence Strategy...
document’s is to update the organisation of national defence in Estonia by taking the changing security environment into consideration, while extending the strategy beyond a strictly military approach to include other areas of national defence which are less traditional.\textsuperscript{117} As the different titles may suggest, the National Defence Strategy takes a much more practical stance to the security issues that Estonia was facing in 2010 and addresses particular courses of action which should be taken. On the other hand, the Concept document provides guidance, goals, objectives and principles regarding Estonia’s security policy and is not designed to articulate how these goals and objectives will be operationalised. The more abstract nature of the National Security Concept corresponds with the metaphorical nature of the concept of resilience. As stated in the literature review, the concept of resilience remains very difficult to operationalise and measure and this is certainly the case within the security context. This could account for the fact that resilience plays such a prominent role in the National Security Concept and not in the National Defence Strategy.

Resilience is viewed as a metaphor or a framework rather than an operational theory or strategy. Figure 5 reveals that the concept of resilience has remained popular in the recent official security documents of the Estonian Government reflecting the wider global security trend. The concept of resilience continues to play a key role in the security rhetoric for numerous Western states and even carries over to powerful international organisations such as NATO and the EU. Resilience was cemented further into Estonian security discourse after NATO committed itself to building resilience at the North Atlantic Council Meeting in Warsaw in 2016: “We are today making a commitment to continue to enhance our resilience against the full spectrum of threats, including hybrid threats, from any direction. Resilience is an essential basis for credible deterrence and defence and effective fulfilment of the Alliance’s core tasks.”\textsuperscript{118} It is a well-known fact that NATO places great weight in the safeguarding of Estonia’s security and this


is demonstrated by Estonia being one of the few NATO members adhering to the requirement of dedicating 2% of GDP to military expenditure.\textsuperscript{119}

In summary, this section has attempted to demonstrate how the concept of resilience has grown in popularity since the 2004 Estonian National Security Concept. Through content analysis the term of ‘resilience’ and associated themes have been systematically tracked through the security documents which has revealed the popularity of the concept (see Figure 5). The research analysis has made a concerted effort to contextualise the results which showed that the increased use of the concept followed the global trajectory of resilience as it has spread in popularity in the field of security.

6.3 Resilience as a Speech Act

In order to gain a better understanding of the use of the concept of resilience within Estonian security discourse, two interview transcripts were examined which provide a deeper understanding of how resilience is conceptualised in Estonia. The first speech act that was analysed was Estonian Prime Minister Jüri Ratas’s speech at the presentation of the 2017 National Security Concept on the 2\textsuperscript{nd} May 2017. The speech took place at the Estonian Parliament (Riigikogu) and the intended audience was thus members of the Parliament. The fact that Prime Minister Ratas was introducing the National Security Concept rather than the Defence Ministry is very telling as it demonstrates the considerable change in the collective security policy mindset from a heavily militarily based approach to a broader approach that takes more aspects of society into account when approaching security.\textsuperscript{120} This is in keeping with a resilience-based approach where civil society is given the responsibility for the security of the community. In that regard it is significant that the Prime Minister highlights in his speech that Estonia’s security environment can be undermined by very different, yet intertwined factors that must be countered with a collective effort where cohesiveness of society is key.\textsuperscript{121} This is an important point to highlight as the cohesiveness of society is an integral component

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{120} Prime Minister Jüri Ratas, “Prime Minister Ratas’s speech at the presentation of the National Security Concept to the Riigikogu”, (Speech, Tallinn, May 2\textsuperscript{nd}, 2017), \textit{Republic of Estonia Government}, Available at: https://www.valitsus.ee/en/news/prime-minister-ratass-speech-presentation-national-security-concept-riigikogu
\item \textsuperscript{121} Ibid
\end{itemize}
\end{footnotesize}
of a resilient nation and something that Estonia can improve. Ratas mentions the term ‘resilience’ for the first time while discussing the sub-chapter on security and the protection of constitutional order. 122 Shortly after the first mention of the concept, the Prime Minister offers a key insight into how resilience is conceptualised by the Estonian Government. He begins by addressing the members of the sitting Riigikogu; “The document you are holding uses a new word, introduced recently to Estonian – kerkusus (resilience). Resilience is the ability of our society to withstand, and recover quickly from, negative impacts and changes. This aspect is dealt with in the sub-chapter on a resilient and cohesive society. Resilience is easiest to achieve in a united society that respects common values; therefore, inclusive, caring and tolerant attitudes, and an appreciation of diversity are becoming more important.”123 The first line of this quote is particularly interesting as it implies that the Estonian word for resilience (kerksus) has only recently been introduced into the Estonian language. This signifies that resilience is not a word with an extensive history in Estonia and its introduction into Estonia could most likely stem from the increased use of the term in the international security context after the 9/11 attacks in 2001. Additionally, the above quote offers a definition of the concept of resilience as the Prime Minister emphasises the need for Estonian society to not only possess the ability to withstand “negative impacts and changes” but also to recover from these events at an accelerated rate. Although brief in its terms, this exert provides us with an opportunity to better understand how the concept of resilience is being developed in Estonia.

The next sample of text that was examined was an interview transcript sourced from Prism, a quarterly journal published by the Center for Complex Operations at National Defence University. The interviewee was Marina Kaljurand, former Minister of Foreign Affairs of Estonia and now Chair of the Global Commission on the Stability of Cyberspace. The interviewer was Michael Miklaucic, the Director of Research, Information and Publications at the Centre for Complex Operation at National Defence University. The audience that this interview aims to target is the readership of the Prism journal who, according to the journal publishers, has expanded to include more than 10,000 officials, servicemen and women, and practitioners from across the diplomatic, defence, and development communities in more than 88 countries.124 The fact that this interview was published in an academic journal and

122 Ibid
123 Ibid
conducted on an Estonian citizen that is no longer an active member of the Estonian Cabinet offers a different perspective of the concept of resilience from the previous speech transcript of Prime Minister Jüri Ratas. The interviewer focused on questions relating to cybersecurity which covered several key talking points within cybersecurity discourse today such as the problem of attribution in cyber-attacks, China’s alternate view of cyber sovereignty and identification of some of the most dangerous developments within the cyber domain. Furthermore, there was a clear Estonian theme throughout the interview given the background of Kaljurand. The interview quickly turns to the subject of resilience as the interviewer asks Kaljurand if she believes that a state should approach cybersecurity by attempting to minimise risks or should accept risks and invest in improving resilience. The interviewee offers a very detailed response as she affirms that multiple elements must be utilised to ensure cybersecurity. Kaljurand highlights that nations must make it as costly and complicated as possible for those who want to attack its systems and she uses the Estonian ID cards as an example, which would cost 60 billion Euros to successfully hack. This deterrence technique which makes the cost of hacking Estonian society extremely high is a form of resilience according to Kaljurand. Studying this transcript reaffirms the notion that the resilience of digital systems is closely connected to the resilience of a nation. Estonia can be viewed as an extreme example of this fact as its reliance on digital systems is amongst the highest in the world. Despite this interview focusing on the role of resilience in the context of cybersecurity, rather than national or societal resilience, it highlights the concepts’ importance across the board in Estonian security discourse. Furthermore, it highlights the strong connection between cybersecurity and national resilience that exists in Estonia.

In terms of concluding remarks for this chapter, it is important to assess what the analysis of the documentation and transcripts has uncovered. The analysis for this chapter focused on the use of content analysis to uncover underlying themes related to the concept of resilience in Estonian security discourse. Resilience has grown in popularity in Estonia over the last fourteen years to an extent where the concept now has its own designated chapter in the last two National Security Concepts. Furthermore, the analysis highlighted that there is a strong connection between the effective implementation of cybersecurity and national resilience in Estonia. The

126 Miklaucic, “An Interview with Marina Kaljurand” p 117.
127 Ibid.
documents assert on multiple occasions the importance of cybersecurity and its role in the continued functionality of Estonian society. Overall, the concept of resilience has been traced through the Estonian security discourse over the last fourteen years and it can be seen that there been a linear acceleration in the influence of this concept over that period. It can be surmised from this analysis that the concept has followed the global trend in terms of the permeation of the resilience concept into the security strategies of several nations.

**Table 1 or Figure 5 : Coding Results of National Security Documents**

<table>
<thead>
<tr>
<th>Document</th>
<th>Resilience (term only)</th>
<th>Protection of Critical Infrastructure</th>
<th>Civil Society</th>
<th>Cybersecurity</th>
<th>Protection of Information Infrastructure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Estonian National Security Concept 2004</td>
<td>0</td>
<td>1</td>
<td>6</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Estonian Cybersecurity Strategy 2008-2013</td>
<td>1</td>
<td>17</td>
<td>1</td>
<td>112</td>
<td>28</td>
</tr>
<tr>
<td>Estonian Long-Term Defence Development Plan 2009-2018</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>National Security Concept of Estonia 2010</td>
<td>18</td>
<td>3</td>
<td>8</td>
<td>9</td>
<td>0</td>
</tr>
<tr>
<td>Estonian National Defence Strategy 2011</td>
<td>1</td>
<td>3</td>
<td>9</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>National Defence</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>
## 7. Cybersecurity and Critical Infrastructure

The previous chapters have established that a tangible link exists between a nation’s resilience and the effective provision of cybersecurity. This chapter is specifically concerned with vulnerability of the energy sector and state agencies to potential cyber-attacks.

### 7.1 Critical Infrastructure

The growing emphasis on critical infrastructure protection is perhaps the most pervasive dimension to homeland security. Critical infrastructure tends to be rather widely defined in

---

the US and the EU, as it officially covers the physical and virtual systems that are seen as of critical importance, such that their incapacitation, disruption or destruction would debilitate valued security referents and systems, including national and economic security and public health and safety. As references are made to critical infrastructure throughout Estonia’s 2008 Cybersecurity Strategy the document includes a list of systems which the Estonian Government considers to be essential infrastructure:

- Energy facilities and networks: electricity, oil and gas storage facilities and refineries, transmission and distribution systems.
- Communications and information technology: telecommunications, transmission and notification systems, software, hardware and networks, including the infrastructure of the Internet.
- Finance: banking, securities and investment.
- Health care: hospitals, health care facilities, laboratories and medicines, search, rescue and ambulance services.
- Food: safety, means of production, wholesale and food industry.
- Water: water reservoirs, water treatment plants and water networks.
- Transport: airports, ports, inter-modal transport facilities, rail and mass transit networks, traffic control systems.
- Production, storage and transport of dangerous goods: chemical, biological, radiological and other hazardous materials.
- State agencies: critical services, facilities, information networks; information systems ensuring national security and defence, resources, databases and court registers with legal effect, and national cultural assets.

This lengthy list provides a valuable insight into what the Estonian Government classifies as essential infrastructure for the functioning of the state. It also acts as a useful reference point to investigate the role that cybersecurity plays in protecting certain aspects of Estonian infrastructure. Security is conceived differently in Critical Infrastructure Protection as the

---


network view of physical and virtual systems means that the key security concepts at play are related not only to protection, but to vulnerabilities and resilience. Thus, the Critical Infrastructure Protection approach to security is closely interlinked with the concept of resilience. These approaches do not strive for total security but instead aim to make risks manageable.

7.2 Energy Facilities and Networks

The importance of the critical infrastructure related to the energy sector is obvious. Estonia is one of the European Union countries that are least dependent on energy imports as they largely meet their energy requirements through the use of oil shale and renewable fuels. That being said, Estonia still remain highly dependent on the operability of its critical infrastructure as the failure its systems could have a devastating impact on the country’s resilience. In 2016 the Estonian Information System Authority (RIA) commissioned a study to map the factors which influence the provision of vital services and it reported that 88% of the Estonian companies surveyed consider the dependency of their vital service on electricity supply as being critical.

In terms of the energy sector, the 2017 Emergency Act provides that during a crisis the Ministry of Economic Affairs and Communications shall organise the continuity of the electricity supply, natural gas supply and liquid fuel supply. The reliance of almost all industries on energy supplies means that almost all sectors have dependence on the energy sector to at least some degree. Notwithstanding the economic risks, the health and well-being of the Estonian people would be placed at serious risk if the energy supply in the country was compromised. As previously mentioned, the increasing reliance of physical infrastructure on ICT has resulted in the importance of cybersecurity reaching new limits. Industrial Control System (ICS) is an umbrella term that refers to a group of process automation technologies such as Supervisory Control and Data Acquisition (SCADA) systems and Distributed Control Systems (DCS).

131 Bourne, Understanding Security, 89.


which concerningly have been subject to a growing number of attacks in recent years. The SCADA systems which are used to gather data and control critical infrastructures, enable engineers to control system components remotely, such as pumps or sluice juice. A diagram is provided at the end of this section that illustrates a typical SCADA system (see Figure 6).

While SCADA systems were originally designed to be closed systems, the number of systems driving critical infrastructure connected to the Internet and interlinked with other systems is increasing each year; and with it the chance for security breaches. Some of the possible security concerns that are associated with the SCADA systems have been identified by Leandros A. Maglaras and his colleagues as there is concern over the difficulties in applying updates, perform patching and modifying system components due to the fact that SCADA must be operational at all times and have long life cycles. Consistent with other resilience based approaches, the risks associated with cybersecurity are never going to be eradicated completely as persistent attackers of SCADA systems will eventually gain access whatever the perimeter protection may be. Vulnerabilities in industrial control equipment are inevitable as it is no longer possible to keep the device cordoned off from the internet, as attackers usually find a way to instigate “attack-ware” in such networks and thus every provider of a vital service must have a backup plan in case the SCADA system becomes unusable. However, these threats can be mitigated by layering security controls so as to reduce the risk to the assets being protected which may not stop competent threat actors but could slow them down and give the protective monitoring service opportunity to alert someone. The serious nature of the consequences associated with a successful cyber-attack on the SCADA systems means that there must be clear protocols and processes for responding to these types of incidents.

---

137 Ibid
138 Maglaras, "Cybersecurity of Critical Infrastructures." 43.
139 Maglaras, “Cybersecurity of Critical Infrastructures.” 43.
141 Ibid
Unfortunately, these types of attacks which target the energy sector and control centres of a country are more likely than simply worst-case scenarios. Power networks are arguably the most important component of all critical infrastructure. This explains why it has become a target of hackers who, through virtual means, can wreak havoc by causing physical disruptions for a nation. An example of a cyber-attack on a nation’s SCADA system can be seen in the case of the cyber-attacks that hit Ukraine in December 2015. Taking control of three Ukrainian electricity distribution companies’ SCADA systems, malicious actors opened breakers at some thirty distribution substations in the capital city of Kiev and western Ivano-Frankivsk region causing more than 200,000 consumers to lose power. These cyber-attacks in Ukraine are the first publicly acknowledged incidents to result in power outages and while the total number of customers that were without power does not add up to a substantial number of customers across the whole of Ukraine, the significance stems from the target selection of the capital city. The attackers demonstrated a variety of capabilities, including spear phishing, variants of the BlackEnergy 3 malware and the manipulation of Microsoft Office documents that contained the malware to gain a foothold into the Information Technology networks of the electricity companies. Although these attacks only caused power outages for a few hours, their destructive element is the first time the world has seen this type of attack against a nation’s critical infrastructure crossing previous boundaries and targeting solely civilian infrastructure. The reason that this example has been included is to demonstrate the potential effect cyber-attacks on Estonia’s electrical supply could have. The attacks that struck Ukraine in 2015 are not exclusive to the Ukrainian critical infrastructure as Estonia could be targeted with a similar attack due to the country’s use of SCADA systems.

Although similar attacks in Estonia, did not have the same effect of the Ukrainian cyber-attacks, Estonian critical infrastructure related to the energy has been targeted in the past showing that harmful actors are prepared to attack the nation’s infrastructure. In 2016, internet traffic bearing the hallmarks of malware was spotted in the computer network of Viru Keemia

144 Ibid
145 Ibid p 23.
Grupp (VKG), an Estonian group of oil shale, power and public utility companies. Software experts found the Mimikatz malware in the VKG office network, used in Windows systems to extract identity credentials (such as passwords, password hashes etc.). A backdoor was also found, used for communication with the control server.\textsuperscript{146} In June 2016, it was discovered that there had been a network connection to the same control server and after further investigation it was discovered that a workstation in the SCADA monitoring segment was infected.\textsuperscript{147} In the Estonian Information System Authority’s (RIA) 2017 annual cybersecurity assessment the report claimed that the malware and control server used have been linked to the APT28 cyber espionage group.\textsuperscript{148} On December 29, 2016 the Department of Homeland Security (DHS) and Federal Bureau of Investigation (FBI) released a Joint Analysis Report confirming the company FireEye’s long held public assessment that the Russian Government sponsors APT28.\textsuperscript{149} This same group has engaged in extensive operations in the name of Russian strategic interests as an example but not limited to, targeting the Organisation for Security and Cooperation in Europe in 2016, Germany’s Christian Democratic Union (CDU) in 2016 and NATO in 2015.\textsuperscript{150} Estonia has to continue to invest heavily in its cybersecurity defence as it significantly bolsters the nation’s resilience to outside attackers. The previous two examples demonstrate the lengths that actors with malicious intentions are willing to go to cause disruption to further their own, and possibly their employer’s, strategic interests.

One way in which Estonia can continue to better prepare themselves for cyber-attacks on their critical infrastructure is by participating in live fire cyber events. In 2010 the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) which is based in Tallinn, launched an event together with the Swedish National Defence College and Estonian Cyber Defence League which has come to be known as Locked Shields. The event has run almost every Spring since as it gives participants the opportunity to learn and test the skills to fend off a real cyber-attack. This year’s event was the largest of its kind with more than 1,000 experts

\textsuperscript{146} Ibid p 24.
\textsuperscript{147} Ibid
\textsuperscript{148} Ibid
\textsuperscript{149} FireEye, “APT28: At The Center of the Storm: Russia Strategically Evolves Its Cyber Operations”, FireEye, January 2017, p 2. Available at: https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf?mkt_tok=eyJpIjoiWlRJNVpUSTBOV1UxWVRNMCIsInQiOiJtNWK2PuSEVDWHMxS0pSdWpydXkZXNdzZhKzdkRXFtbGhjQmtGMTR6ZDZ3ZhOhitRQzhmUEVJT2Fb0wQmZrRFlwTWYyUDJ2cnJxK0Jca3ljQ2lwVHRUMUdPY2toK1IwMIFEWTNzMVNycFM0M1IaS21BdzFqV3VoY2xiaSJ9 (Accessed May 2018)
\textsuperscript{150} Ibid 4.
from thirty countries taking part in the exercise.\textsuperscript{151} Locked Shields 2018 had a clear theme as the main aim was to rehearse the protection of different vital services and military systems in the event of a large scale cyber-attack. Aare Reintam, the head of the exercise at the CCDOE said that in light of the cyber threats that have been identified of late, participants in this year’s exercise are being offered the opportunity to rehearse protecting various vital services, civilian and military systems. In accordance with the scenario of the exercise, participants must be able to protect the system against cyber-attacks targeting the power grid, 4G public safety networks, a water purification station and control systems of military drones.\textsuperscript{152} Exercises like this give nations an invaluable opportunity to test themselves against some of the world’s experts in cybersecurity and provides them with a chance to tackle one of the biggest security threats to modern societies today. Besides from the networking opportunity, it gives the computer emergency response team (CERT) of participating countries the ability to be better prepared if a cyber-attack on their nation’s critical infrastructure occurs. Specifically, in terms of Estonia, the fact that the exercise is held every year in Tallinn reaffirms the idea that this small nation is one of the world leaders in cybersecurity. Improving the skills and experience of Estonia’s CERT boosts the resilience of Estonian society no end as it will be in a much better position to respond to cyber-attacks on critical infrastructure such as Ukraine experienced in 2015.

7.3 State Agencies

This section addresses another aspect of critical infrastructure that relates to the role of ‘State Agencies’. This concerns the protection of vital services that make the logistical running of the country possible such as: information systems ensuring national security and defence; resources; databases and court registers with legal effect; and national cultural assets. Government agencies are particularly popular targets for cyber espionage, in which external threat actors such as state-affiliated organizations or nation states infiltrate networks looking for sensitive data. According to RIA’s 2017 Annual Cybersecurity Assessment government institutions were involved in between 20-30\% of all cyber incidents in 2016, with the Estonian


\textsuperscript{152} Ibid
CERT registering 1,687 cyber events related to government sector institutions.\textsuperscript{153} As to cyber risks in the public sector in Estonia, the two areas that are most at risk are the operational continuity of the information systems that support other public services or national security, and, attacks mounted with the aim to defraud or with political or ideological motives.\textsuperscript{154} As with most cases in cybersecurity, actors with sinister intentions attempt to compromise Estonia’s public sector by targeting the weakest link in the defensive chain, the human element. Malicious actors utilise social engineering techniques such as phishing, spear-phishing, water holing and baiting to target public servants in order to gain a foothold into the Estonian governmental systems. As this dissertation has briefly touched upon, Estonian society is considered as one of the most digitised in the world. The nation claims that 99\% of public services are available to citizens as e-services such as i-Voting, e-Residency, e-prescriptions, e-Health Records and e-identities which allow citizens to access all of Estonia’s e-services.\textsuperscript{155} Due to almost all of Estonian Government services and their databases being managed online, Estonia is particularly dependent on the functionality of its information systems. During the interview with Marina Kaljurand which has already been cited in the previous chapter of this thesis, the former Minister of Foreign Affairs was questioned about Estonia’s reliance on e-government and the potential to make the country more susceptible to cyber aggression. Her answer was that Estonia was more vulnerable because of its reliance on internet services but at the same time it forced the country to improve its cybersecurity and maintain its position as Europe’s number one in cybersecurity.\textsuperscript{156}

Asides from promoting greater awareness of cybersecurity in Estonian society, one of the most valuable and innovative ways that the Government has increased its cybersecurity and therefore resilience, is through the use of data embassies. As Estonia’s “paperless governance policy” has been implemented it has meant that essential databases only exist in digital form. If a situation arose where a major natural disaster, cyber-attack or terrorist attack hit Estonia, the process of securing this digital data could present a major issue. The Estonian Government has devised this innovative data embassy solution which involves placing Estonia’s systems and data in another sovereign country, as it creates an additional security guarantee for Estonian

\textsuperscript{154} Ibid 21.
\textsuperscript{156} Miklaucic, “An Interview with Marina Kaljurand” p 119.
sovereignty. Estonia will back up critical data and services important for the functioning of the state outside the physical territory of Estonia as they launched the scheme in partnership with the Government of Luxembourg in 2017.\textsuperscript{157} The data embassy scheme is the first of its kind and has the potential to benefit Estonian citizens who will be the recipients of a more reliable and secure digital society and it also creates an extra security guarantee for 30,000 or more e-residents who expect Estonian digital services to be available at any time independent of location.\textsuperscript{158} It must be highlighted that the data embassy initiative is not in operation yet but the Riigikogu passed the legislation that would allow Estonia to host its critical databases in Luxembourg from February 2018.\textsuperscript{159} Luxembourg was chosen as a hosting partner because it has state-owned high security data centres that have been certified at Tier 4 level - a centre that is fault tolerant, allowing for the occurrence of any unplanned activity while still maintaining operations.\textsuperscript{160} It is still not clear how the concept is going to operationalised as of this month, no action plan or requirements have been established for the implementation of the concept and additional measures agreed upon for the protection of critical databases have not been officially determined in any document.\textsuperscript{161} However, the innovative agreement with Luxembourg has significant potential with other countries expected to join the scheme in the future. Estonia’s dependence on digital systems has been well documented in this thesis and any solution that reduces the risks associated with this dependency are a positive. Thus, the data embassies are yet another method in which cybersecurity increases the national resilience of Estonia.

This chapter has examined a select number of ways in which cybersecurity is utilised to protect the critical infrastructure of Estonia. Out of the list of nine critical infrastructures that the Estonian Government have designated, cybersecurity plays a role in the protection of every single sector. The functioning of critical infrastructure is one of the fundamental components

\begin{footnotesize}
\begin{enumerate}
\item Ibid p 44.
\end{enumerate}
\end{footnotesize}
of a resilient nation and cybersecurity ensures that this critical infrastructure remains operational.

A typical SCADA system (Figure 6)\(^{162}\)

---

\(^{162}\) Maglaras, “Cybersecurity of Critical Infrastructures.” 44.
8. Cybersecurity and Civil Society

The final issue to be examined in this thesis is the nexus between cybersecurity and civil society, as it plays a prominent role in Estonia. The chapter will be divided into three sections with the initial subsection establishing the connection between civil society and resilience. The second section will use the Estonian Defence League Cyber Unit for the purposes of examining the interaction between cybersecurity and civil society. Finally, consideration will be given to the strong tradition of inter-agency cooperation in the cybersecurity community of Estonia.

8.1 Civil Society and Resilience

There is a consensus that civil society represents an intermediary sphere, a kind of buffer zone between individuals’ micro worlds and large institutions. In this respect, the intermediary sphere is constructed from a string of organisations and associations, the so called “third-sector”163. This sphere is important from a democracy point of view as well as for the sustainability of social cohesion.164 Scholars such as Vlasta Zekulić, Christopher Goodwin and Jennifer Cole have claimed that when dealing with contemporary security challenges it requires a whole-of-government and whole-of-society approach. Civil preparedness for crises is critical in sustaining overall defence because the effective delivery of force and military capabilities relies on resilient civilian resources.165 Here, civil society is given the responsibility for the security of the community and functions as part of republican liberal notions of civic virtue and duty, in which the national/homeland interest is asserted but not debated and the state enables and facilitates others to provide security while evading ultimate responsibility for it.166 This idea of the dispersal and reconfiguration of security roles has its roots in Cold War defence practices, as during this time there was an emphasis on civil preparedness as national unity of effort and civil preparedness walked hand-in-hand with military readiness.167

164 Ibid
166 Bourne, Understanding Security, 90.
However, the aforementioned authors highlight that the security environment has changed since the Cold War and therefore the system of resilience from that time cannot be resurrected. Instead they claim that renewing national resilience against contemporary threats requires a cross-governmental and comprehensive approach, re-invigorating civil-military cooperation, and creating the support systems that understand the deep interdependencies between, the military, civil and private sectors.\footnote{Ibid 33.} If we briefly refer back to Figure 3 from the work of Norris et al, which illustrates the networked adaptive capacities, two of the four network adaptive capacities which are closely related to civil society in Estonia are “Social Capital” and “Community Competence”. From the ‘Social Capital’ node shown on Figure 3, there are three sub-capacities that emerge which closely relate to the cohesiveness of the society, namely, ‘attachment to place’, ‘sense of community’, and ‘social embeddedness’ (see Figure 3). If one is to accept this line of thinking from Norris and her colleagues, then these three factors are integral for a resilient nation. Separately, as will be demonstrated in the next section, collective efficacy and empowerment, political partnerships and community action are aspects of the Community Competence Node identified by Norris et al that have been developed in Estonia.

It is not only academics who have acknowledged the importance of civil society as an essential component of national resilience as policy makers have also begun to recognise this fact.

In Estonia, the concept of civil society has been intimately connected with the promotion of democracy, including above all participatory democracy. The concept followed the general Western conceptualisation of the term and the belief that civil society is both needed and realisable in Estonia.\footnote{Risto Alapuro, “Russian and Estonian Civil Society Discourses Compared”, in in: White S. (eds) Media, Culture and Society in Putin’s Russia. Studies in Central and Eastern Europe. (Palgrave Macmillan, London, 2008) 14.} Today, the nation of Estonia greatly values the importance of civil society. For national resilience to become an important operational concept for Estonia it is fundamental that there is unity between the state and civil society. In the Estonian case this is particularly applicable as the Government relies on the civilian sector to support the Estonian Defence Forces in the defence of the state.\footnote{Estonian Ministry of Defence, National Defence Strategy Estonia 2011, 2011, p 14.} The 2011 National Defence Strategy states that the civil sector’s support to military defence shall be ensured by mobilisation, the utilisation of state assets, contractual relations and compulsory encumbrances.\footnote{Ibid} This reaffirms the Estonian
government’s approach to defence and society as demonstrated by the following from the Estonian Ministry of Defence official website:

“National defence comprises more than just military defence. One can contribute to national defence by non-military means which strengthen the bond between a citizen and the state, help develop the defence will of the nation and therefore strengthen the principles of action and sovereignty of the state.”

The Estonian Defence League is a part of the Defence Forces, a voluntary militarily organised national defence organisation operating in the area of government of the Ministry of Defence. The unit of particular importance to this study is the Estonian Defence League’s Cyber Unit which is another voluntary organisation aimed at protecting Estonian cyberspace.172

8.2 Cybersecurity-Civil Society Nexus

This section aims to illustrate the role that cybersecurity plays within civil society in Estonia. The Estonian Defence League is a part of the Defence Forces, a voluntary militarily organised national defence organisation operating in the area of government of the Ministry of Defence. The unit of particular importance to this study is the Estonian Defence League’s Cyber Unit which is another voluntary organisation aimed at protecting Estonian cyberspace.173 The Estonian Defence League Cyber Unit can be categorised under the sub-capacity of “citizen participation, leadership & roles” (see Figure 7). Estonia has enjoyed a long-standing national ICT security cooperation among commercial, governmental and academic bodies. Against this background, the cyberattacks Estonian information infrastructures that accompanied the 2007 spring ‘Bronze Nights’ protests met a collaboration network already in place; and indeed, the horizontal collaboration between private and public sector information security experts was generally viewed as a major factor for successfully handling the attacks.174 In 2009, two cyber defence sub-units were created in Tartu and Tallinn, as part of the corresponding regional units of the Estonian Defence League. In 2011, these regional sub-units were re-assigned and formed

into the Estonian Defence League Cyber Unit (CDU). Furthermore, the project was envisioned by the community as an instrument to offer meaningful contribution to cybersecurity, and it met well with the expectation of the Cyber Security Strategy to identify and develop forms of collaboration and communication among the various stakeholders involved. In this respect, as a small country Estonia has an edge over bigger countries - the small size of its cyber security community and the limited number of state authorities responsible for ensuring cyber security produce favourable conditions for easier private-public cooperation. This has helped to create a real civic feel within the cyber community in Estonia as the smaller size of the sector makes it a more personal sector to work in compared to bigger nations such as the UK and the US. This is further evidence of Estonia demonstrating innovative skills in relation to the cyber security field as the CDU is, yet another example of how cyber security can be utilised to boost national resilience.

Although CDU members are not automatically obliged to take part in the activities of the unit, there appears to be a strong appreciation and paid staff of the organisation for the members’ commitment to participate in the organisation. Due to the nature of the organisation, members are usually recruited among valued professionals and with strong manifested cyber skills and often hold demanding jobs with their employer and participate in the activities of the Unit alongside their work commitments and without receiving compensation. This makes one question the motivations of volunteers for this organisation as they do not receive remuneration. The CDU’s umbrella organisation the EDL was one of the subjects of Silva Kiili’s 2015 study which investigated the motivations of joining the Estonian Defence League, The Estonian Defence Forces and the Danish Home Guard. As can be seen from the rankings, the personal values of the participants were grouped into ten motivational value types

178 Ibid 18.
179 Ibid.
The leading motivational group was security for the Estonian Defence League (see Figure 7) under which the highest scores were assigned to family security, national security and self-respect. This gives an insight into why Estonia citizens become involved in civil society organisations and in particular, organisations related to voluntary territorial security. Although this provides a general overview of the motivations of Estonian volunteers, it is important to look at the specific motivations for the CDU. Arguably the biggest incentive for joining the CDU is the training that it provides for its volunteers as the organisation has provided a number of seminars, information sharing and training events as well as field studies since 2010. Another important factor is the civic duty aspect of the organisation as volunteers must feel as though they are carrying out important tasks and therefore positively contributing to the national security of Estonia. For an organisation like the CDU to be successful, the members must be trusted to carry out meaningful tasks related to national defence for the CDU to positively contribute to building the national resilience of Estonia.

The identified objectives of the Cyber Defence Unit centre around three main themes:

a) developing a network of cooperation, including for crisis response. This is sought by strengthening cooperation among qualified volunteer IT specialists as well as by the creation of a network to combine the expertise of public and private sectors to act in crisis;

b) improving the security of critical information infrastructure by raising the level of security of critical information infrastructure, both through regularly sharing threat awareness and disseminating best practices as well as enhancing preparedness for operating during a crisis situation;

c) promoting awareness, education and training both by providing continuous information security education and training to members as well as actively participating in cyber security training networks, including international ones.

The first objective of the CDU is closely related to one of the fundamental characteristics of the concept of resilience. The ability of a society to withstand an external shock may it be physical or virtual, and then recover and adapt is the mark of a resilient society. In accordance

---

181 Ibid 5.
with the Emergency Defence Act, the Estonian Defence League may be used in the prevention of objects with a high risk of attack.\textsuperscript{184} The Act does not specifically identify the potential role, once engaged, of the Defence League in general or the Cyber Defence Unit in particular; authorisation is given to the Government of the Republic on a case-by-case basis.\textsuperscript{185} This means that the CDU can be mobilised during a crisis to assist the official Estonian CERT if the country comes under attack in the cyber realm and can contribute to the defence of the nation’s critical information infrastructure. This increases the relevance of the CDL compared to traditional military units, which are typically limited to the protection of military systems.\textsuperscript{186} The organisation’s second objective of improving the overall security of information infrastructure in Estonia is achieved by the expertise that the volunteers bring to the organisation as it creates a stronger front for the Estonian nation to fight or resist and deter cyber warfare. Furthermore, one of the advantages of this organisation is that it a relatively cost-effective way of building a highly skilled and specialised reserve force.\textsuperscript{187} The third objective of the CDU corresponds with one of the four-year goals of the latest Cyber Security Strategy which proclaims that it aims to increase the population’s cyber security capabilities and raise awareness of cyber threats, thereby ensuring continued confidence in cyberspace.\textsuperscript{188} The CDU can be utilised to provide continuous information security education to Estonian society by providing external training and awareness raising events. In 2011-2012 the CDU held eight cyber defence seminars for governmental institutions.\textsuperscript{189} By increasing the overall awareness of cyber security within Estonian society the country is ensuring that is more cyber resilient against cybercrimes and cyber espionage. Furthermore, it is important for Estonia to promote cyber security awareness as its title as Europe’s most digitalised nation demands this. Overall, the CDU is one of the most effective means by which the Estonian state bolster its national resilience through cyber security and this is closely connected to successful inter-agency cooperation.

\textsuperscript{184} Ibid 24.
\textsuperscript{185} Ibid.
\textsuperscript{187} Ibid 779.
\textsuperscript{189} Kaska, Osula, Stinnissen, “The Cyber Defence Unit of the Estonian Defence League”, p 22.
8.3 Inter-agency Cooperation

Historically, although there has not been a defined public-private partnership for cyber security in Estonia, the Information System Authority operates in close cooperation with the private sector. However, in January 2018 the Estonian Information Security Association was formed which brings together academia, the private sector and the Estonian Government in the form of the Ministry of Defence and Estonian Information Systems Authority. Founding members feature leading Estonian cybersecurity companies (BHC Laboratory, Clarified Security, Cybernetica, Guardtime) and esteemed academic institutions, including Tallinn University of Technology and Tartu University in respect of which the joining process is ongoing. The agreement formalises existing cooperation between enterprises, research institutions and government agencies as the agreement lays the foundation for further cooperation across sectors and focus areas ranging from particular technologies to macro problems such as data integrity, cyber capacity building and hygiene as well as skills development. These types of public-private partnerships (PPPs) are often seen as the ‘answer’ to many of the challenges related to cybersecurity governance: PPPs are, in policy as well as academic circles, often considered as a mode of organisation that can enhance flexibility and robustness by including a broader range of civil and private actors. Strategic EU documents on cybersecurity repeatedly emphasise the role of PPPs and private-sector collaboration in combating cyber-attacks and cyber-crime. Similarly, the Estonian strategic documents, in particular the 2014-2017 Cyber Security Strategy stresses the importance of public-private sector cooperation.

There has been criticism of this approach to cyber security from academics, such as Madeline Carr, who claims that one of the major stumbling blocks is that:

---

192 Ibid
193 Ibid
195 Ibid 1438.
“What is in society’s best interest with regard to cybersecurity is not always in the best interests of the private sector. This is because, they argue, social benefits do not translate in terms of private profitability—no matter how desirable the outcome.”

She claims that this disjuncture in perceptions is arguably at the heart of the tension in this ‘partnership’. However, authors such as Kristoffer Kjærgaard Christensen and Karen Lund Petersen have argued that while there is some truth in this observation, it tends to overstate a particular historically bound meaning of utility (and economic) interests, and to overlook the role of loyalty and commitment to more general moral principles. They argue that it is important to acknowledge that the concept of corporate risk and security has widened in recent years; there is an increasing tendency to think of corporate security in wider social and political contexts, for example through corporate social responsibility, sustainability policies and reputation management. The close personal relationships within the cyber community in Estonia amongst individuals in both the private and public sphere, makes Kjærgaard Christensen and Lund Petersen’s argument even more convincing. This particularly resonates with the Estonian case as Estonian experts believe that voluntary contribution to cyber security in the country is primarily based on goodwill and enthusiasm of individuals. Although there is potential for significant problems to emerge out of the public-private partnership in Estonia in relation to cyber security, the inter-agency cooperation of these sectors has so far proved to be successful. The inter-personal relationships that exist in the Estonian cyber community could be considered unique to Estonia due to the small size of the country and the well-developed expertise in cybersecurity. Successful public-private cooperation in the field of cyber security in Estonia is essential in ensuring that cybersecurity bolsters the national resilience of the country.

To conclude, the role of cyber security within civil society is a fundamental tool that is utilised effectively to build resilience within society. This thesis has already documented the effects cyber security can have on the resilience of a nation and through organisations such as the CDU and public-private cooperation, Estonian citizens have the chance to contribute to the national

198 Ibid
200 Ibid
defence of Estonia. In 2018 cyber security is an integrated part of national defence for Estonia and the inclusion of civil society in this field should be viewed as a way to increase national resilience.

(Figure 3)
9. Findings and Conclusion

To conclude, arguably the most important finding from the research carried out for this thesis is that a clear nexus exists between cybersecurity and national resilience. In Chapter Five the critical analysis of the cybersecurity – national resilience nexus demonstrated that in the contemporary security environment where the concepts of national resilience and cybersecurity have been securitised by Western countries such as Estonia, a strong tangible link exists. Through the use of content analysis, it was discovered that both concepts featured heavily in the official security documentation of the Estonian Government. In relation to cybersecurity, Estonia’s attempts to securitise the sector after the infamous 2007 attacks garnered partial success. Although the nation failed in its attempt to convince its NATO allies to invoke Article 5 in response to the attack, the nation’s portrayal of the event led to the further securitisation of cybersecurity in the international arena. The concept of resilience has also been securitised by the Estonian Government through the use of speech acts, including an elite declaration by
the Prime Minister Juri Ratas, who has discussed the concept in one his addresses to the Estonian Parliament. The Prime Minister addressed the need for a resilient approach to security threats and defence in the country. The concept of resilience has followed the wider international trajectory of the concept as its use was very limited before 2010 but has seen an exponential rise in academic study and security policy making since this date. The concept of resilience now features as a key concept in the official National Security Concept of Estonia which outlines the approach to security that the nation is planning to undertake.

After the nexus between cybersecurity and national resilience was proven, the next objective of the thesis was to examine how the concepts interacted within a national security context. Critical Infrastructure Protection is an approach to security which is closely connected to the resilience concept as the successful maintenance of critical infrastructure during a crisis, is a key component of a nation withstanding an external shock or stress. The research focused on the energy sector and the functioning of state agencies, both important components of critical infrastructure. The analysis demonstrated that with the increased digital connectivity of critical infrastructure in developed countries in 2018, cybersecurity played a key role in the operability of these systems. This section also demonstrated that claims that the cybersecurity sector has been securitised without just grounds are unfounded. The discussion made use of the 2015 Ukrainian cyber-attacks to prove that malicious actors now have the capabilities and willingness to attack vital services and infrastructure that pose a threat to human life. This findings from this chapter demonstrated to the researcher that a nationally resilient Estonia is not possible without effective cybersecurity measures and structures in place. Although the nation’s title as the world’s ‘most wired’ country brings numerous benefits, it also makes Estonia more vulnerable to cyber-attacks. This makes the nation an appealing target for malevolent actors who can fully appreciate the devastating effects a successful cyber-attack could have on ‘e-Estonia’. This chapter of the dissertation proved to offer some of the most stringent evidence that cybersecurity bolsters the national resilience of a nation.

The final research question which was devised for this thesis examined the relationship between civil society, cybersecurity and national resilience. It is generally accepted that without the existence of a strong civil society movement, it is not possible for a nation to achieve a true resilient standing. The Estonian case study provides a unique example as
organisations such as the Estonian Defence League Cyber Unit, a volunteer civil organisation, combine civil society with cybersecurity as their main objective to help defend Estonian cyber-space. The findings from this research demonstrated that the role of cyber security within civil society is a fundamental tool that is utilised effectively to build resilience within Estonian society. This thesis has already documented the effects cybersecurity can have on the resilience of a nation and through organisations such as the CDU and public-private cooperation, Estonian citizens have the chance to contribute to the national defence of Estonia. In 2018 cybersecurity is an integrated part of national defence for Estonia and the inclusion of civil society in this field should be viewed as a way to increase national resilience.

In conclusion, this thesis has proven that cybersecurity has a positive effect on bolstering the national resilience of a nation. As Estonia was chosen as a most likely case, if the results of this research had demonstrated that cybersecurity has the potential to erode the national resilience of the country, then cybersecurity could not be considered as a mechanism to strengthen the national resilience of a nation. This research has demonstrated that cybersecurity has a significant impact on a nation’s national resilience and this thesis would go as far to claim that in a country such as Estonia, who rely so heavily on digital systems, the manifestation of national resilience is not possible without cybersecurity. However, one last caveat must be added to this statement. Although this thesis has proven that cybersecurity is an essential component in building national resilience in Estonia, this is not necessarily the case for other nations. Estonia possesses a unique set of characteristics, namely, the country’s dependence on digital systems, the small size of the nation and its superiority compared to most nations in the cybersecurity sector. These factors have combined to create a unique scenario where cybersecurity is a key component in bolstering the national resilience of Estonia. Further studies should be undertaken to examine the effect that cybersecurity has on the national resilience of larger nations such as Germany or the US, or perhaps, countries who do not possess the same cyber capabilities as Estonia.
Bibliography

Books

- Bourne, Mike. Understanding Security, (Basingstoke, Palgrave Macmillan, 2014),
- Young, Thomas. A course of lectures on natural philosophy and the mechanical arts, (London: J Johnson Publishers: 1807)
Journal Articles

MSc SECINTEL Independent Study (Dissertation)


News Articles

- FireEye, “APT28: At The Center of the Storm: Russia Strategically Evolves Its Cyber Operations”, FireEye, January 2017, p 2.Available at: [https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf?mkt_tok=eyJpIjoiWlRJNVpUSTBOV1UxWVRNMCIsInQiOiJqTnlWK2FuSEVDWHMxS0pSdWpydUxkZXNDdzZvKzdXRkFtbGhjQmtGMTR6ZDZ3SzhObitRQzhmUEVJT2FPbk0wQmZrRFJwTWYyUDJ2cnJxK0Jaci3iQ2IwVHRUMUdpY2toK11wMlFEWTNzMVNycFM0M11aS21BdzFqV3VoY2xiasSJ9](https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf?mkt_tok=eyJpIjoiWlRJNVpUSTBOV1UxWVRNMCIsInQiOiJqTnlWK2FuSEVDWHMxS0pSdWpydUxkZXNDdzZvKzdXRkFtbGhjQmtGMTR6ZDZ3SzhObitRQzhmUEVJT2FPbk0wQmZrRFJwTWYyUDJ2cnJxK0Jaci3iQ2IwVHRUMUdpY2toK11wMlFEWTNzMVNycFM0M11aS21BdzFqV3VoY2xiasSJ9) (Accessed May 2018)


Websites

- NATO, “Resilience and Article 3”, NATO, June 2016. Available at: https://www.nato.int/cps/ic/natohq/topics_132722.htm (Accessed May 2018)


Official Documents

