Cybersecurity

- Determinants of cybersecurity policies -

Student name: Dennis van den Berg

Student ID: 402551db

Location: Erasmus University Rotterdam

Academic year: 2013-2014

Department: International Public Management and Policy (IMP)

Supervisor: Michal Onderco

Number of words: 27.492

Date: 28-08-2014

Abstract

Cybersecurity has been put high on the agenda's of most countries around the world. This research analyzes the determinants of cybersecurity policies of 23 countries partner to the NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE). For this end a Country Analysis Model is developed which ranks countries based on three dimensions; legal foundation, agency responsibility, and international cooperation. The countries are analyzed primarily on the data put forward in the National and Cyber Security Strategy documents. Although cybersecurity is a primary concern of the countries the development of their cybersecurity policies differs significantly. The determinants used for the analysis are technological development, internet penetration, and military expenditure. The approach taken by the governments included in the CCDCOE database is highly diverse and is related to the perspective in which cybersecurity is held. The determinants are tested with the use of a linear regression to find which is most significant for the determination of cybersecurity policies.

Keywords: cybersecurity, policy, strategy, NATO

Table of content

List of figures and tables

Table of abbreviations

Abbreviation	Definition
APEC	Asian-Pacific Economic Cooperation
Budapest Convention	Council of Europe's Convention on Cybercrime
CCDCOE	Cooperative Cyber Defense Centre of Excellence
CERT	Computer Emergency Response Team
CSS	Cyber Security Strategy
DDoS	Distributed Denial of Service
E-commerce	Electronic commerce
E-government	Electronic government
GDP	Gross Domestic Product
GovCERT	Government Computer Emergency Response Team
ICT	Information and Communication Technology
IP	Internet Penetration
IP address	Internet Protocol address
IR	International Relations
ME	Military Expenditure
NATO	North Atlantic Treaty Organization
NCSC	National Cyber Security Centre
NCSS	National Cyber Security Strategy
NSP	National Security Policy
NIST	National Institute of Standards and Technology
SDA	Security and Defense Agenda
Sigint	Signals intelligence
TD	Technological Development

1. Introduction

Cybersecurity is a subject which is increasingly receiving more attention. The attacks on government and private institution's websites in Estonia in 2007 and the cyberattacks on the Georgian government in 2008 have been important for this. The attack even convinced the NATO to place their cybersecurity research centre in Tallinn (The Economist, 2008). As NATO Secretary General Rasmussen stated at the 2013 Defense Ministers meeting "cyber-attack are getting more common, more complex, and more dangerous. They come without warning. From anywhere in the world. And they have devastating consequences" (NATO, 2013).

Attempts to protect countries against unwanted intrusions in their cyberspace are becoming more frequent and countries are increasingly more aware of the threats. For example, the NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE) was officially opened in 2009. Furthermore, the 2012 Security and Defense Agenda (SDA) report, in collaboration with McAfee, ranked countries according to their cyber defense. No country acquired the highest score of 5, however, Finland, Israel and Sweden shared the first place with 4,5 out of 5. Denmark, Estonia, France, Germany, the Netherlands, Spain, the United Kingdom and the United States all were awarded with a 4. The lowest score was given to Mexico, which acquired 2 out of 5 (Grauman, 2012).

The past attacks and these scores tell us very little given that they do not indicate why some countries have developed more than others. Rather, the McAfee ranking takes into account the protocols and programs a country uses, without looking into the determinants for cybersecurity policies. Therefore, the reasons and motivations that drive countries to have a strong set of cyber defense policies remain unresolved.

The protection of critical infrastructure and the potential harm of a cyberattack have led to the implementation of new policies and the construction of various cyber defense agencies in many countries around the world. Additionally, a gradual shift is visible which has changed military strategies in order to account for potential adverse effects of cyber activity.

However, strong disagreement exists about the nature and effects of cyber risks and potential attacks, which has resulted into fragmented policies and the absence of a coherent cybersecurity framework. Countries have benefited from the positive effects of various forms of e-government and other aspect of the internet without timely realizing the need for effective and well-established policies to guide the digital practices (Kello, 2013; Mueller, Schmidt, & Kuerbis, 2013; Sharma, 2010).

This research will determine which factors are the main determinants of country's cybersecurity policies with the use of a statistical analysis. However, research in the field of cybersecurity is fairly limited and hence the first part of this research is aimed at providing the reader with a general understanding of cyberspace and its different components. Overall, the aim is to find the determinants of cybersecurity policies and therefore the research question is:

"Which factors determine the level of development of a country's cyber security policies?"

Cyberspace influences the daily lives of billions and the use of the internet has been expanding ever since its introduction. Cyberattacks have a potential damaging effect on individuals, companies and governments alike. The attacks impact these actors in various ways given that they all have increasingly come to rely on the use of cyberspace. This reliance on cyberspace is the reason why potential attacks are a concern for those using it. The use of the internet has significant benefits and has led to increased efficiency rates. According to Katsikas (2005) in the European Union up to 30 percent of the increased efficiency can be attributed to 'web-enabled services'.

Today, cyberspace can be used for nearly anything, from daily groceries to the functioning of a country's critical infrastructure, such as its electricity network. Furthermore, an increasing amount of personal data is exchanged and provided over the internet. Nevertheless, the abuse of cyber technology is "expanding the range of possible harm beyond the traditional conceptions of war and that it poses new challenges for national and international security" (Kello, 2013, pp. 38). The novel identity of cyber technology and the potential adverse effects form the foundation of this research. The aim is to find out how cyberspace has changed the conventional military perspectives of countries and the reasons for implementing their respective cybersecurity policies.

For this end, within this research first of all which factors influence a country's cybersecurity policies will be statistically analyzed. Secondly, the Netherlands and Denmark will be thoroughly analyzed with a case-study research to illustrate the differences in military perspectives with regards to cybersecurity. However, before conducting this research chapter 1.1 will introduce cybersecurity and elaborate on some of the most prevailing theories and ideas about contemporary cybersecurity. Chapter 1.2 will provide some different perspectives on cybersecurity as not all scholars agree on the potential risks of cyberattacks. Following this, chapter 1.3 will clearly define the terminology used within this thesis to guide the reader through the maze of different terms and concepts.

Chapter 2 is concerned with security policies in general and cybersecurity policy in particular. Therefore, chapter 2.1 will illustrate how national security policies are made. Paragraph 2.2 addresses the security dilemma in relation to cybersecurity. Paragraph 2.3 will continue and show how these general policies are translated into cybersecurity policies. The final paragraph of chapter 2 will highlight which determinants have been identified as most important and consequently will be used as independent variables in the quantitative analysis.

Chapter 3 explain the method used within this research. The units analyzed will be discussed in paragraph 3.1. Following this, paragraph 3.2 explains the Country Analysis Model with its three different dimensions – legal foundation, agency responsibility, and international cooperation. Paragraph 3.3 elaborates on the independent variables used with paragraph 3.4 explaining the method of analysis used; multiple linear regression. The last chapter concerns the case-study design. Overall, chapter 3 explains the dependent and independent variables and the general research set-up will be provided to explain how the data has been found and the research conducted.

Chapter 4 is concerned with the individual analyses of the countries under scrutiny, which are included in appendix G. Paragraph 4.1 provides a summary of the analyses and rigorously investigates the findings. Additionally, paragraph 4.2 is concerned with the relation between the implementation time of the Budapest Convention and the level of cybersecurity policy development for the individual countries. Chapter 5 interprets the data based upon the SPSS data output, with the first chapter describing the assumptions which are to be met for a multiple linear regression. The following paragraph uses Cronbach's Alpha to determine the international consistency of the developed model, and hence scale reliability. Paragraphs 5.3 to 5.5 are concerned with the statistical analysis of the data for each of the different dimensions of the Country Analysis Model. Finally, the limitations of the study will be summarized in paragraph 5.6

Two countries have been investigated more closely; the Netherlands and Demark. The findings are presented in chapter 6. These countries are expected to have a different approach with regards to cybersecurity policies but are relatively similar with regards to socio-economic, political and organizational set-up. All the information presented in this research is summarized in chapter 7. Finally, Chapter 8 discusses some of the limitation for this research.

1.1 Cybersecurity

This research analyzes the cybersecurity policies pursued by governments and the effects of

cyber risks on government security policies. Lehner, Miller and Wonka (2007) argue that "social relevant research furthers the understanding of social and political phenomena which affect people and make a difference with regards to explicitly evaluative standards" (pp. 27). Cybersecurity is often addressed by technologists, nevertheless, its people who utilize the cyberspace and hence they are an important part of cybersecurity (Kello, 2012). According to Gartzke (2013), political science and international relations can be useful to critically assess the policies and actors involved in cybersecurity. Currently, International Relations theory or political science approaches are virtually absent in the field of cybersecurity. Nevertheless, much can be gained when examining the implications of the information age on international security and international relations.

Furthermore, although research from private companies is publicly accessible, these findings are primarily concerned with the technical properties – as is the case with McAfee. For that reason, analyzing what the impact is of cyberattacks and other digital malicious behavior on policies developed by countries is beneficial to gain new insights (Kim, Wang, & Ullrich, 2012).

Therefore, this research will analyze the level of sophistication of cybersecurity policies pursued by governments and determine which factors shape this level of development. Thereby enhancing the knowledge of cybersecurity in general and aiding future cybersecurity research from a political science perspective. Furthermore, the case-study of cybersecurity policies of Denmark and the Netherlands will investigate whether or not cybersecurity has resulted into changes in conventional military strategy or rather reflect the current status quo just with new instruments at government's and other actor's disposal.

Another important aspect to be considered is: "How does an issue become a security problem?". The concept of securitization, arguably one of the most prominent theories coined by the Copenhagen School of Security, is a helpful tool to explain the efforts made in the area of cybersecurity. Cybersecurity has been approached more comprehensively, with an increasing focus on international cooperation (Zwolski & Kaunert, 2011). According to Buzan, Waever and de Wilde (1998) two main perspectives on security studies are visible today; the traditional state-centered view and the new view of the 'wideners'. Traditionalists broadly "equate security with military issues and the use of force" (pp. 1). Whereas the wideners take a more comprehensive approach and include nonmilitary factors as well. By incorporating 'an ever wider range of issues' in the security sector the term runs the risk of become void and meaningless for international relations.

The authors continue by arguing that the conceptualization of security must go beyond

mere threats and vulnerabilities; these are present in both military and nonmilitary areas, however, to be considered as a security problem clearly defined criteria have to be met. First of all, the problem must be considered as an existential threat. For the military sector, which is the area in which cybersecurity is regarded, "the military security concerns the two-level interplay of the armed offensive and defensive capabilities of states, and states' perceptions of each other's intentions" is important. This leads to the question: "to which view to states adhere with regards to cybersecurity?".

The NATO CCDCOE members and partners, as explained below, have declared cybersecurity to be a priority. Furthermore, the summit in 2012 and the commitments expressed indicate that cybersecurity is considered to be an international security issue. The reason for this classification can be found in the traditional understanding of security, with a focus on military and political implications. This view holds that states seek survival; the means to achieve this is through security given that security is primarily concerned with survival. When a phenomenon or problem is portrayed as an 'existential threat to a designed referent object', in this case a state, can a problem become an international security issue. The NATO members have issued a joined report indicating the threats cyberspace poses and are seeking cooperation within this field. Furthermore, the members consider cyber threats to be potentially detrimental to a nation's daily functioning (NATO, 2012).

As Admiral Mullen puts it "the single biggest existential threat out there, I think, is cyber" (NATO, 2014). Therefore, the NATO members see cyber threats and cybersecurity in the traditional military-political perspective and are expected to respond with behavior and actions related to this view (Buzan et al., 1998). Chapter 1.2 will elaborate on the different perspectives currently noticeable with regards to cyberattacks and cybersecurity in general. With the use of a literature review different perspectives from some of the most prominent authors in the field of cybersecurity and international relations will be given and the differences highlighted.

1.2 Different perspectives on cyberattacks

Contemporary international security is mostly focused on states and interstate relations. Nevertheless, some authors argue that non-state actors have the ability to use the cyberspace to negatively affect states and interstate relations. As Nye (2012) puts it "the barriers to entry in the cyber domain are so low that non-state actors and small states can play a significant role at low cost" (p. 1). The 'empowerment' of non-state actors is one of the new concerns for

decision- and policy-makers. The increasing reliance on cyberspace for governments creates unprecedented vulnerabilities and requires comprehensive and well-researched policies (Kello, 2013; Nye, 2012).

The consequences of cyberattacks are disputed and the implication of a large scale attack is subject to different theoretical beliefs. Furthermore, whether or not 'the era of cyberwar has already arrived' is disputed (Gartzke, 2013, pp. 41). Some scholars, which Gartzke (2013) frames as 'cyber pessimists', argue that recent events, such as the attack on the government websites of Georgia and Estonia, on which a Distributed Denial of Service (DDoS) attack was launched, demonstrate that cyber warfare has already significantly advanced as a contributive tactic. Other examples are the hacking of the digital military networks of the United States and the Stuxnet worm, which was targeted at the nuclear centrifuges in Iran. For these scholars the striking aspect of cyberattacks is the fact that they can be targeted at Western governments and civilizations.

Attacking the technological instruments of a developed country is significantly different from conventional war tactics, which for at least the past 70 years, have been against insurgents or perceived rogue states. The military equipment used often was inferior to that of its Western enemies and hence the battles were asymmetrical as a result of the unequal military technologies (Gartzke, 2013; Kello, 2013; Nye, 2012). Therefore, scholars such as Nye (2012) and Kello (2013) argue that the increasing usage of cyberspace and cyber systems for a wide range of activities, from economic activities, to critical infrastructure and military systems, "creates new vulnerabilities in large states that can be exploited by nonstate actors" (Nye, 2012, pp. 1).

Overall, the number of threats is increasing whereas the source of origin is often uncertain. This is a problem for states given that without a known perpetrator it is highly difficult to take countermeasures or engage in retaliatory behavior. Furthermore, next to the new threats facing nations and individual users, traditional forms of criminal behavior are being transferred to the digital domain, thereby increasing the problem. Additionally, it is impossible to completely secure the digital domain (Katsikas, 2005; Cavelty, Mauer, & Krishna-Hensel, 2007).

Cavelty, Mauer and Krishna-Hensel (2007) argue that "the decreasing costs and increasing performing power of computers have led to the application of information technologies (IT) in virtually all corners of society" (pp. 3). Moreover, the increased interconnectedness and technological developments pose unprecedented difficulties. Cyberspace transcends borders and is intangible; causing unawareness for both the public and

private sector. Governments are increasingly transferring activities to the digital domain. According to cyber pessimists, the risk associated with this development is significant and continuously expanding. Therefore, “the risk environment transcends the limits of time and space boundaries, and presents a continuous and general challenge (…) they affect all users, transactions, and dataflows regardless of location or political persuasion” (Cavelty, Mauer, & Krishna-Hensel, 2007, pp. x).

The increasing awareness of problems with the use of cyberspace is also visible internationally. The first official widespread international attempt to monitor and regulate cyberspace is ‘The Convention on Cybercrime. This Convention was adopted on November 23, 2001 by the Council of Europe and aimed to “set up a fast and effective regime of international cooperation”. The Convention is open for members and non-members of the Council of Europe. Nevertheless, even though 41 countries to date have ratified the Convention, 11 countries have not, among them members of the Council of Europe (Council of Europe, 2014; Kim, Wang, & Ullrich, 2012).

Contrary to the above, other scholars have argued that cyberattacks are more a secondary tactic, serving a supportive role to ‘terrestrial military violence’. Cyberwar or attacks do not constitute the new type of warfare, given that they cannot replace ground troops or equipment. Another aspect decreasing the importance of cyberattacks stems from the international relations concept called the ‘shadow of the future’. For scholar such as Gartzke (2013) “for threats or demands to prove effective, targets must believe both that an attack is likely to follow from noncompliance and that the attack is destined to inflict unacceptable harm” (pp. 42).

What the paragraph above indicates is that cyberattacks are often considered to be a side-effect of using cyberspace. Cyberattacks are not seen as catastrophically, rather as costs associated with contemporary activities (Katsikas, 2005; Fischer, 2009; Gartzke, 2013; Walt, 2010). The view or classification of cyberattacks is a determining factor in the attitude of states. Additionally, whether or not cyberattacks are considered to be a means in itself is likely to influence the policies pursued by states. The next chapter will illustrate which view is held by most states under scrutiny in this article.

The costs associated with a high level of cybersecurity have to be weighed against the harm, both potential and currently experienced. Therefore, critics of the potential effects of cyberattacks argue that without the ability to cause ‘substantial durable harm on an adversary’, cyberattacks will not become the crucial part of grand military strategies. Rather, cyberattacks should be considered as a potential first strike, nevertheless, conventional

military forces will have to follow up in order to cause devastating damage. Overall, cyberattacks will serve a supportive role, used in conjunction with other types of attacks; it creates a 'window of opportunity' for an attack using see, air or land forces (Katsikas, 2005; Fischer, 2009; Gartzke, 2013; Walt, 2010).

Any government in the world is faced with many possible threats. Nevertheless, it is impossible and undesirable to protect against everything. Government budgets are inherently finite and hence the available funds to counter cyber threats are limited (Katsikas, 2005). Therefore, upon deciding which policies to pursue countries will have to balance the perceived threat. Finally, international relations theory illustrates that increasing cyber capabilities, as with traditional means of protection, will not necessarily result into a safer society. As Gartzke (2013) puts it "the risk of attack is never zero, given that a potent defense or deterrent endangers the security of others" (pp. 51).

Before diving deeper into cybersecurity and its different aspect and dimensions, the terminology must be made clear. Despite the fact that there is not global agreement on the concepts, the concepts explained below and their definitions will be used throughout this thesis.

1.3 Defining cybersecurity terminology

The plurality of the terms used in the field of cybersecurity means that a clear defining line is often absent; different words for the same meaning and terms without a clear definition are widespread (Cavelty, Mauer, & Krishna-Hensel, 2007). Given that the field of cybersecurity is relatively new and only recently started to get attention, it is crucial to clearly define what is meant with the terms used within this thesis.

First of all, the area in which this topic takes place is called cyberspace which is exploited by an internet user. An internet user can be defined as someone who utilizes "the publicly available worldwide system of interconnected computer networks that transmit data by packet-switching using a standardized interconnection and transport protocol and many other protocols" (OECD, 2005). Secondly, cybersecurity "consists of measures to protect the operations of a computer system or the integrity of its data from hostile action" (Kello, 2013, pp. 18). Generally speaking, a cyber-attack is "unauthorized intrusion into computer systems and their proper functioning" (Kello, 2013, pp.18).

For this research, all types of attacks, including but not limited to viruses, worms, Trojan horses, spyware and DDoS attacks will be taken into account (Arquilla & Borer,

2007). Cyberwarfare is different from cyberattacks in general. Cyberwarfare, further elaborated below, will be used to describe an attack, or set of attacks aimed at either "degrading an enemy's military capabilities; penetrating networks to shut down civilian infrastructure; web-based criminal activity; or cyber espionage" (Walt, 2010, pp. 1).

Overall, the different types of cyberattacks can be divided into two big subgroups; offensive and defensive activities (Cavelty, Mauer, & Krishna-Hensel, 2007, pp. 22). For the scope of this article this distinction will be mainly used. However, there are also distinctions within these two groups. In essence there are five main concepts discussed in cybersecurity literature; cybercrime, cyber terrorism, cyber activism, cyber espionage, and cyberwarfare (Dutch Ministry of Security and Justice, 2011; Rueter, 2011; Clarke & Knake, 2011). These categories overlap to some extent and hence the distinction is not always clear. The key factor can be found in the origin, or source of the attack. The analysis is concerned with the actors behind a specific attack and the purpose they have.

The first type of cyber threat is cybercrimes. These are executed by individuals, or small groups of individuals, which are often motivated by financial gain, notoriety or by the mere 'challenge of circumventing security measures'. These types of hackers, from hereon called cyber criminals, are most often not a military problem or concern. Cybercriminals do sometimes attack government servers, however, not significantly more than business or private systems. Therefore, although cybercrimes are unwanted and can potentially disrupt the proper functioning of servers and systems, they are not the primary concern for governments and their military (Clarke & Knake, 2011; Rueter, 2011).

The second category is cyber terrorism, which are attacks carried out for ideological reasons. Cyber terrorists can use the same means or portray the same behavior as cybercriminals, nevertheless, the motivations and goals are significantly different. Cyber terrorism, according to Clarke and Knake (2011) is a subjective concept as it creates images of 'Bin Laden waging cyberwar from his cave' and this type of attack has not been visible since 2012 (Hathaway & Klimburg, 2012). Nevertheless, the distinction is necessary for the reader to get a comprehensive idea of the concepts currently used.

The third category, cyber activism or 'hacktivism, is often considered as a subcategory of cyber terrorism. These are attacks motivated by ideological behavior but with less rancorous intentions. Fourthly, cyber espionage has become more frequent in recent years. Today, cyber espionage is expected to be widespread and entails 'spying for political or military gain'. This is different from the previous categories where the motivations were personal. Cyber espionage is a concern for governments and the military because crucial

information can be stolen. It is important to note that cyber espionage can be used for cyberwarfare, however, cyber espionage in itself does not constitute cyberwar (Clarke & Knake, 2011; Rueter, 2011).

Cyberwarfare, the final category, is different from activities carried out by criminals or terrorists for the reason that this is primarily the domain of states. This is a crucial difference, given that not individuals or small groups but states are the actors and the source of origin. Cyberwarfare can be broadly defined as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption" (Clarke & Knake, 2011, pp. 11). Finally, cyberspace itself should be considered as a separate domain, a distinctive dimension from the traditional areas of air, land space and sea. Rather than conventional types of warfare, cyberwar does not take place in a physical battlefield (Clarke & Knake, 2011; Hathaway & Klimburg, 2012; Rueter, 2011). Despite the lack of agreement on terminology the distinction described above will guide the reader throughout this thesis.

This research focuses on deliberate malicious digital behavior with the aim of suspending the proper function of a country's critical computer systems. Therefore, the attacks on industry, private corporations or individuals will not be investigated. The goal is to seek which policies are pursued by governments both offensively and defensively and how these are influenced by cyber threats. The next chapter will illustrate how security policies are broadly made. The reason for this is that it can be used as a comparison for the way in which countries make cybersecurity policies. Although no country is the same, there is some general overlap in security policies and hence this will be the foundation to build upon.

2. The policy process

An important question to answer before focusing on the determinants of cybersecurity policies is: "How do countries make decision about security policies?". Before the determinants of policies in general, and cybersecurity policies in particular can be analyzed, the decisions which precede policies have to be analyzed. Most countries have a national security policy (NSP). This is a framework or strategy and describes the methods, policies and other tools used to provide security to a nation's citizens and state structures.

Most countries have first made general national security policy documents, which often included some broad statement on cybersecurity. However, as the previous chapters illustrate, cybersecurity has become a primary concern for most countries. This has resulted into the creation of cybersecurity policy documents in which the issues are given separate attention. These national or issue specific documents are used within this research to determine which cybersecurity policies the countries have implemented. For this end the documents provided by the NATO CCDCOE will be used.

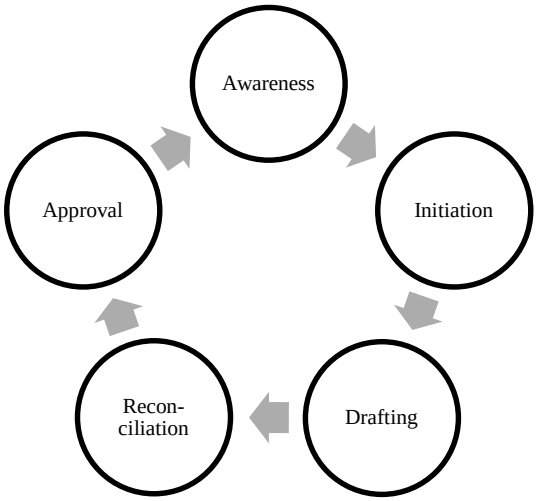
An example of how NSP documents can result into cybersecurity policy documents is given in appendix B. The table shows the documents of some of the biggest NATO members and those countries which have a specific focus on cybersecurity; the United Kingdom, Germany, Canada, France, the United States, Australia and the Netherlands. The evolution of national security goals into specific cybersecurity goals will be discussed in chapter 2.1. This chapter will explain how national policy documents are made and why they are important for cybersecurity policies. First of all, a general overview of a policy cycle will be given; this will aid the reader into broadly understanding how policies are made. The chapter will continue by connecting cybersecurity and the overall national security policies.

A NSP document is not in all countries an integrated document and thus should be considered as an overarching term to describe the strategies, plans and decisions made by a country in the area of security. For example France and the United Kingdom do not have one integrated NSP document, although these countries have so-called 'White Papers' these are somewhat different from NSP because they are not solely authoritative documents but also serve the role of stimulating public debate. Additionally, these white papers are often less detailed or only issue specific rather than an overall coherent document. Nevertheless, for comparison reasons, the white papers will be used as the guiding documents of these countries and hence will be included in the analysis later on (DCAF, 2005).

The NSP has both a current and prospective or future function. Security policy gives form to the main interest of a country. Furthermore, a NSP sets guidelines 'for addressing current and prospective threats'. Generally, the NSP takes precedence over specific policies such as homeland security or military strategies. Therefore, as cybersecurity targets a specific issue as well, a NSP is hierarchically superior.

Broadly speaking a NSP covers three main topics. First of all, the role of a country within the international system and its vision thereof determines which policies are pursued. Secondly, the perceived opportunities and challenges of a country both with regards to the international system and domestic threats. However, much of the focus is spend on international preferences and security partners. Finally, the third theme revolves around the responsibilities and response to the perceived challenges and opportunities in specific areas (DCAF, 2005).

Figure 1: Simplified policy cycle



A common simple policy cycle consists out of four main processes; initiation, drafting, reconciliation and approval (Hathaway & Klimburg, 2012). This is a simplified cycle as most often the process is stalled or stopped because agreement cannot be reached or the situation has changed. Nevertheless, as this research is not concerned with a policy cycle itself this simplified version will be used. Furthermore, one step is added – awareness – which refers to the official declaration or priority given to a specific issue. As the previous paragraph illustrates, most governments have declared cybersecurity to be an important topic and awareness has been raised. This awareness is necessary for the policy cycle to be set in motion given that policies are only created when a 'hot topic' is put on top of the agenda.

Thus, awareness of a specific issue or threat is necessary before the policy process starts. Although the terms differ between authors, the general method is the same. The initiation phase is usually handled by the executive, sometimes supported by the legislature or expert groups. Additionally, the drafting of a security policy text falls under the responsibility of the executive, or a subgroup thereof such as specific committees; which can be either an ad hoc or a standing body. Reconciliation referrers to the process where input from different stakeholders and actors are involved and used during the process. Finally, approval may be required by the executive or legislator for the endorsement of the document (DCAF, 2005).

The cycle discussed here is a simplified version and should not be taken as a strict model given that it differs from country to country and between governmental systems. The purpose of this paragraph is to give an indicative view, some context to the reader when thinking about policy making and the reasons for having a specific set of policies. For this research the reason for having a specific set of cybersecurity policies is analyzed and hence the policy cycle broadly explains how these policies are developed. This is helpful to give some perspective as to how security policy is made because a similar process is required for the formulation of cybersecurity policies.

States regard security as one of the most important issues. Nevertheless, security in many areas is often inadequate, both the standards set and quality delivered. The security systems used are often unsuccessful in protecting the institutions and systems used. Even in the public sector governments and security officers often only have ‘a limited interest in enhancing security’. Button (2009) argues that “the delivery of security is frequently delegated to personnel with limited training, inadequate education and no real commitment to professionalism” (PP. xv). Therefore, it is important to find out “Which factors determine security policies?”. The following paragraph will elaborate on the factors involved in security policies and focus on cybersecurity policies in particular. The findings, in turn, will be used for the field of cybersecurity in the next paragraph.

Bayuk (2010) uses ‘triads’ to describe the usage and objectives of cybersecurity policies. First of all, the prevention, detection and response to cybersecurity are crucial for the achievement of effective mechanisms. Prevention is one of the primary goals of any security plan; to prevent disruptions in systems and successful attacks. Nevertheless, as discussed above, it is impossible to prevent all attacks given the opportunities adversaries have. Therefore, detection of and response to attacks are vital for an effective cybersecurity regime. The detection and response is directly affected by the laws and regulations developed in a

country and the agency structure implemented. Consequently, these two aspects will be used in the analyses of the countries.

The second triad used concerns people, processes, and technology. These concepts are important for any technological field in general, and hence, for cybersecurity in particular. The key factor is that people, in this case security professionals, cannot achieve security on their own. It only takes one person to allow malicious users of the internet access to a system. On the other hand, good process and a high level of technology used are not sufficient either.

Consequently, an effective security program has to take into account all factors and include the fact that other elements and decisions made are essential for the success of a security program. Overall, it becomes clear that cybersecurity requires comprehensive cooperation with all relevant stakeholders. As a result, countries will have to cooperate internationally as cyberspace transcends borders and cannot and its security cannot be secured by a single country (Bayuk, 2010). International cooperation will be one of the dimensions in the analysis section.

Finally, next to effective mechanisms and critical technological and human factors, confidentiality, integrity and availability are important. Although these concepts play a significant role, they are often contradictory. Making information available can undermine the confidentiality thereof. This is one of the reasons why countries are hesitant to report the number of attacks. Additionally, the integrity of information, in essence the authenticity and accurateness of information reported and recorded, can be undermined based upon the confidentiality and availability. Overall, for each sector, system and organization these factors have to be weighted and hence require a case-by-case decision (Bayuk, 2010).

So far it becomes clear that once awareness is raised and government officials have declared an issue to be important the policy process is set in motion. The following chapter goes further and will establish the reasons for making an issue a priority. Additionally, the factors which determine a policy will be made clear. Chapter 2.1 further elaborates on cybersecurity policies and how these are made.

2.1 Cybersecurity policies

Bayuk et al. (2012) describe cybersecurity policy broadly as a policy “adopted by a governing body and formally applies only to the corresponding domain of governance” (pp. 7). What this indicates is the lack of a coherent overarching framework in the field of cybersecurity. The stakeholders involved depend on the scope and field in which the policy is proposed or

adopted. Nevertheless, governments of states are increasingly adopting policies which apply to all citizens and companies active in their territory.

Naturally, the scope and content of a cybersecurity policy depends on the aim of the governing body of that country. Therefore, countries such as Estonia and Georgia which have been subject to attacks, or countries such as the Netherlands and Germany with open, export-oriented economies are likely to adopt different policies based on past experiences and potential effects on their other economic, political or social policies.

The previous chapter talked about NSPs and the creation of these documents. Today, most governments are formulating National Cybersecurity Strategies (NCSS). These are kept relatively broad because "governments, business, and citizens know intuitively that cyberspace is man-made and an ever-expanding environment, and that therefore the definitions are also constantly changing" (Hathaway & Klimburg, 2012, pp. 9).

The strategy paper of the United Kingdom's government of 2009 can be taken as an example. The document states that "cyberspace encompasses all forms of networked, digital activities; this includes the content of and actions conducted through digital networks" (UK Cabinet Office, 2009, pp. 7). Hathaway and Klimburg (2012) describe the process from governments for the formulation of cybersecurity policies (see appendix A).

The process is rather similar to the policy cycle discussed chapter 2.0. First of all, the importance is stressed for the initiation of policies. Thus, governments articulate 'the need for information assurance', 'information security', 'implementing computer security' or any statement similar to these. The concepts are used interchangeably; the important aspect is the expressed need to defend the cyberspace against unauthorized intrusions. After the articulation the policy process starts. Nevertheless, not all countries agree on what constitutes cybersecurity.

The Dutch NCSS (2011), similar to the UK NCSS, defines it broadly as "freedom from danger or damage due to the disruption, breakdown or misuse of ICT" (pp. 4), and aims to include the five categories of cyber threats mentioned above. The International Organization for Standardization on the other hand has a more narrow view and "defined cybersecurity as the preservation and confidentiality, integrity and availability of information in the cyberspace" (Hathaway & Klimburg, 2012, pp. 12). These examples show the increasing awareness and action taken by governments to define cybersecurity within their

national strategy reports and documents. The statements will serve as the first stage of investigation of the cybersecurity policies pursued by governments[1].

Separate from cybersecurity in general is the use of cyber defense. The defense part most often indicates military involvement and hence goes beyond the scope of mere cybersecurity of Information and Communication Technology (ICT). For example, the NATO, which the majority of the countries analyzed are a member of, uses two definitions for the information security environment. One is aimed at the broader area of systems related to communication and information and in which cybersecurity "is defined as the ability to adequately protect the confidentiality, integrity and availability of Communication and Information Systems (CIS) and the information processed, stored or transmitted".

Whereas cyber defense "is the ability to safeguard the delivery and management of services in an operational CIS in response to potential and imminent as well as malicious actions that originate in cyberspace" (Hathaway & Klimburg, 2012, pp. 12-13). The difference between the terminologies might indicate a difference in policies, as this research will analyze, however, for now the importance lies in the commitment shown by the different countries and organizations to protect national defense and the cyberspace, including critical infrastructure and information used.

The articulation is only the first step; the realization or awareness that policies are necessary. Awareness in general, and articulation in particular, lead to the first stage, the initiation; the beginning of a policy. An NCSS would merely constitute the end-product, or approval stage. Therefore, the drafting and reconciliation stage require some attention. Three dimensions are important for an NCSS; governmental, national and international. Most countries have difficulties with determining which ministry or department is responsible. Given the extensiveness of cyberspace and the use thereof, many departments can claim responsibility.

Consequently, the NCSS must take account of increased cooperation and interaction between the different departments within government and there is a necessity to take a 'whole of government' approach. This requires significant effort and clear and comprehensive policies and divisions of tasks. Additionally, national actors involved include anyone from security companies, to private firms and the general public. All of these actors are involved in cyberspace (Hathaway & Klimburg, 2012).. As a result, the agency responsibility structure within a country is important to effectively protect its cyberspace. If responsibility is shared

[1] See an excerpt of 7 OECD Countries in Appendix C; For an overview of the statements from 50 different OECD countries see Hathaway & Klimburg, 2012

across many different departments and clear authority is absent the effectiveness of a country cybersecurity framework is limited. Therefore, agency responsibility will be used as one of the three dimensions in the analysis section.

Finally, there is the international dimension; the inherent feature of cyberspace is that it transcends borders and hence international cooperation and collaboration with a wide-range of international partners is necessary. Cybersecurity requires countries to exchange knowledge and information. Furthermore, as international cyber legislation is highly limited countries will have to agree upon common approaches. All these dimensions and the actors active therein have to be considered and to some extent included in the drafting and the reconciliation stage of an NCSS (Hathaway & Klimburg, 2012).

Cybersecurity policy is most often not considered as a separate field, rather as a subcategory of a nation's general national security policies. This is a critical factor in the determination of policies. If cybersecurity policy is considered to be as important as for example economic, social or foreign policies the outcome would be highly distinct than when it is part of a countries military strategies of national defense policy. It is important to note that although not all countries have specific laws for the field of cybersecurity this does not indicate a lack of policies. Even though adopting regulations or national laws would grant cybersecurity more official legal force policies are also articulated with the use of speeches, reports or formal statements.

As Bayuk et al. (2012) mention "it is possible to have cybersecurity executive directives, laws, and regulations without have articulated cybersecurity policy at all" (pp. 7). Therefore, for the determination of a country's cybersecurity policy it is important to not solely focus on legal documents. Overall, when determining which cybersecurity policies are in place the focus should not solely be on formal policies. The reason for this is the fact that security decisions will be made, even if not formal policy is visible. Consequently, the legal foundation dimension will take both formal and informal policies into account in the analysis section.

Chapter 2 and 2.1 illustrated the policymaking process and illustrated some of the main dimensions of a comprehensive cybersecurity framework. The central question in this research is 'which factors determine the level of development of a country's cybersecurity policies?'. Three main dimensions have been highlighted; legal foundation, agency responsibility, and international cooperation. These dimensions will be used in the analysis section in order to determine the current level of development or maturity of the different country's cybersecurity framework.

2.2 Cybersecurity and the security dilemma

A major difficulty for cybersecurity is the fact that the distinction between offensive and defensive capabilities is highly blurred. For example, professional hackers can both defend and attack systems. This has as a result a high level of uncertainty of other state's intention which increases mutual distrust. Consequently, deterrence is highly problematic in the area cybersecurity.

One of the problems is the traceability, in this case the determination of where an attack originated from as discussed in chapter one, is very limited. Even if an IP address is traced, something which is not always possible if a hacker uses multiple fake addresses, it is still unclear for governments if this originating from individual hackers or government employed hackers. Deterrence often relies on ' the threat of credible punishment', nevertheless, countries may understandably decide not to publically punish an cybercriminal as this can expose weaknesses in national system or undermine international credibility (Farrell, 2014; Lynn, 2010).

Thus, characteristics of cyberattacks make the likelihood of overcoming the security dilemma difficult. Additionally the traceability or attribution of cyberattacks further increases the problem because identification of the attack or source is problematic. Furthermore, terminology and definitions used are worrisome. There is no universal agreement on what constitutes a cyber weapon or how likely specific attacks are. Which is, as discussed above, one of the reasons why NCSS's are kept relatively broad (Hathaway & Klimburg, 2012; Rueter, 2011).

The article by Robert Jervis (1978) is concerned with anarchy and the security dilemma. In this article Jervis argues that the anarchic nature of the international system makes international cooperation less likely. However, for an issue such as cyberspace, which transcends borders, cooperation is of crucial importance, and will be one of the dimension of the policy development model used in this research.

The logic of the security dilemma holds that states are uncertain about each other's intentions. Additionally, increasing national defense capabilities can result into a reinforcing interaction with other states and has the possible consequence of war, even if not actual aggressive behavior is sought by any state. The above paragraph illustrated that a problem exists with the distinction between offensive and defensive capabilities, which in turn leads to uncertainty. According to Farrell (2014) these notions have an impact on cybersecurity

policies of states. This is a result of the difficulties associated with the protection of cyberspace; computers, technology and people have inherent weaknesses and soft spots.

Therefore, Farrell argues that “it is far easier to attack others’ information systems than it is to defend one’s own” (pp. 1). Thus, offensive capabilities preside over defensive capabilities. The significance of the security dilemma is the fact that an effective cybersecurity policy requires international cooperation. States will have to cooperate in order to secure their cyberspace as it transcends borders and cannot solely be addressed as a domestic issue. International cooperation will be discussed as one of the independent variables in chapter 3.

Kello (2012) distinguishes some main implications for international relations. The diffusion of power as a result of the ability of non-state actors to execute cyberattacks has increased the number of potential adversaries. Nevertheless, the prevailing notion is state-centered and ‘security is still conceived in national terms’. This poses a problem as effective reactions requires a rethinking of concepts.

As stated above, it is almost impossible to determine whether an attack is supported by government, hence the boundaries between private and public actors are disappearing. For example, China is known to employ large numbers of civilian hackers. Furthermore, there appears to be a legislation gap. National laws and regulations are often not adapted to respond to malicious cyber behavior, and individual hackers are highly unlikely to ‘comply with interstate rules’.

Overall, the most prevailing problem is the increase of uncertainty; stable patterns can be disrupted as a result of the attribution problem, making the creation of effective cybersecurity policies a complex matter (Kello, 2012). The attribution problem feeds into another issue, the dependency problem. Governments increasingly rely on multiple forms of electronic government and commerce, from here onwards e-government and e-commerce.

The usage of e-governance and e-commerce is widely embraced by both the public and private sector. These types of electronic behavior require trust, stable patterns and expectations to be used to its fullest potential (Hathaway & Klimburg, 2012). However, international cooperation and reliability are undermined by the cyber threats discussed in chapter one. What this indicates is a reconsideration of cybersecurity policies and the ideas behind them.

Hathaway and Klimburg (2012) argue in their report from the NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE) that there are five mandates of national cybersecurity; military cyber, counter cybercrime, intelligence and counter-intelligence,

critical infrastructure protection and national crisis management, cyber diplomacy and internet governance. These mandates correlate with the above mentioned dimensions of cyber threats. The military cyber dimension is concerned with cyberwarfare, and the increasing capabilities of countries in this field. This dimension looks at cybersecurity as the fifth dimension, next to land, air, space, and sea capabilities.

Secondly, counter cybercrime addresses criminal web-based activity. This includes hacktivism and cyber terrorism which is where the importance lies for this analysis. The third dimension, intelligence and counter-intelligence, concerns cyber espionage. Critical infrastructure protection is relevant in as much as national crisis management has to take into account the cyber dimension in the future, given that future crises are expected to be connected to cyberattacks.

Finally, diplomacy, as the name indicates, is aimed at international cooperation and setting of standards. This is, as mentioned before, crucial given the inherent international nature of cyberspace. These dimensions will be taken into account in the determination of the policies executed by governments later on (Hathaway and Klimburg, 2012).

2.3 From national policy to cybersecurity policy

The theories discussed above indicate the increasing awareness and preoccupation with cybersecurity. This section will illustrate the development of national security policy and to which extent these national policies accommodate cybersecurity defense. For this chapter two countries have been chosen to illustrate the development; Denmark and the Netherlands. The reason for using these countries is the fact that these will be subject to a case-study later on and that they are helpful in explaining the different stages in which the policy processes are in the different countries.

The Danish government reached an agreement in 2012 on their defense plan for the years 2013-2017. The report mentions that “The continued proliferation of weapons of mass destruction and long-range missiles, as well as the threat in cyberspace from governmental and non-governmental actors alike, represent an increasing security risk for Danish society and the Danish armed forces (pp. 2).

In the Danish report cybersecurity is discussed together with other possible threats. Additionally, throughout the rest of the agreement cybersecurity is often discussed together with threats in the Arctic; both considered as newly emerging threats. Later on in the defense plan the government states that “the defense must have the capability for military operations

in cyberspace, including the ability to protect own network infrastructure, and also to affect opponents' use of cyberspace" (pp. 4).

The government aims to increase its Centre for Cybersecurity, which is headed by the Ministry of Defense. Overall, around 65 million DKK have been allocated in 2013 to accommodate the cybersecurity development. This example shows that cybersecurity has moved away from solely one aspect of national security policy towards a more separate issue. Although the cybersecurity is discussed both separately and in conjunction with other possible threat in the Defense Agreement, the government has not issued a report or reached an agreement on cybersecurity as completely separate topic. The Danish government aims to have a well-functioning centre and hence military defense capabilities.

Contrary to Denmark, the Netherlands has issued several cybersecurity reports and action plans. The latest, the 2013 "National Cyber Security Strategy 2" report extensively discusses cyber threats and capabilities. The report aims to move beyond mere awareness and towards tangible response mechanisms (National Coordinator for Security and Counterterrorism, 2013). The first report was an assessment of the most prevalent threats and risks for the Dutch and international cyberspace. With the 2013 report and the separate discussion of the topic, the Netherlands appears to be further in the decision making process when compared to Denmark.

Additionally, the report mentions that "with this strategy, the Netherlands wants to continue to be the world leader in the area of cyber security" (pp. 3). The importance of this statement is two-fold. First of all, the Netherlands considers itself to be a leader in cybersecurity and aims to further increase its policies. This outspoken attention and effort in the area of cybersecurity is absent in the Danish national report. Rather than viewing cyber threats as relatively novel, the Netherlands focuses on improved response mechanisms.

Overall, the Netherlands appears to have moved away from general national security policies towards specific cybersecurity policy, whereas, Denmark regards cybersecurity in a more conventional view – as part of the national military strategy.

2.4 Key determinants of cybersecurity policies

This chapter will discuss three determinants which have been identified as crucial in the contemporary cybersecurity paradigm. The determinants chosen are: internet penetration, in essence the number of internet user per 100 inhabitants; military expenditure as part of a country's GDP; and the level of technological development of a country. These three

determinants have been chosen based on the above literature review and theoretical framework.

Admittedly, more determinants can be thought of, such as the number of internet exchange points, the number of attacks a country encounters, the size of a country's services sector, and the total use of e-governance to name a few. Nevertheless, these three determinants are considered pivotal based upon the literature review. Furthemore, the scope of this research does not allow for the inclusion of all these aspects. Finally, the other determinants are less likely to influence cybersecurity policies and are therefore not used in this research. The reason for choosing these three as the key determinants will be explained below as well as the reasons for not choosing other potentially plausible determinants.

2.4.1 Technological development

Most authors agree that a devastating attack or 'an electronic or cyber pearl harbor', at least in the near future, is unlikely (Fritz, 2008; Gartzke, 2013). However, Weimann (2004) argues that "the growing dependence of our societies on information technology has created a new form of vulnerability, giving terrorists the chance to approach targets that would otherwise be utterly unassailable, such as national defense systems and air traffic control systems. The more technologically developed a country is, the more vulnerable it becomes to cyberattacks against its infrastructure" (pp. 2). Nevertheless, as Weimann points out, highly technologically developed countries have a higher potential risk. The assumption is that these countries are more focused on increased cybersecurity policies and advanced protocols. Therefore, technological development is the first key determinate.

Furthermore, the amount of money and funds used for the development of cybersecurity measures requires a certain level of technological development. The knowledge and funds required are therefore expected to relate to the level of cybersecurity development. The countries used in this research are therefore primarily developed countries. Most of the countries in the sample have established knowledge sharing platforms, centers of excellence or cooperation agreements. An effective cybersecurity framework requires collaborations between governments, the academic sector and the industry. For this end a stable political situation is favorable and hence the countries under scrutiny are primarily stable democracies (Ralston, Graham, & Hieb, 2007).

An alternative to technological development could be to focus on economic development or the country's size of the services sector relative to the production sector.

However, the services sector includes a wide range of activities, many of which may not be conducive to the cybersecurity sector. Next to this, economic development would not be specific enough variable. Further reasons for choosing technological development will be discussed in more detail in chapter 3.3.1.

2.4.2 Internet penetration

Pivotal in the relationship between internet penetration and cybersecurity is that the greater the reliance on internet the greater the need is to improve cybersecurity. The rationale behind this is based on the notion that most of the governmental policy documents concerned with cybersecurity start with the assumption that the increased usage of cyberspace, in particular the internet, has resulted into an increased vulnerability and must be met with proper countermeasures as explained in the previous chapters and more rigorously in the country analyses. Therefore, countries with a high internet usage are expected to put the issue higher on the agenda when compared to other nations. Overall, countries with a high internet penetration are expected to have a more rigorous cybersecurity framework.

The United Nations Office on Drugs and Crime (UNODC) has calculated the average and total 'costs of cybercrime'. From the study, one tendency becomes visible when comparing the relative numbers. "Where large differences arise, one contributing factor may be differences in internet penetration and distribution of costs across society" (UNODC, pp. 30). As differences in internet penetration can be linked to differences in costs per capita governments with high levels of internet penetration are expected to be more affected by the costs rather than other, often less developed countries, with a lower internet penetration rate.

The study by the UNODC shows that in countries where some part of the population has no access to the internet the average suffered costs per capita due to cybercrimes is lower compared to countries in which the majority of the population has access to the internet. In countries with internet penetration rate the reported individual losses are more similar to the estimated losses. On the other hand, in countries, mostly highly developed countries, the losses from cybercrimes are higher than estimated consumer losses, indicating other costs from 'indirect and defense costs' (UNODC, 2013, pp. 30). What this indicates is that in countries with a high internet penetration the average costs are higher.

The inherent 'nature' and free access to the internet causes some concerns. This is why governments with a high level of internet users are expected to be more concerned with increasing their cybersecurity frameworks. The more internet users, the more a country

becomes dependent on interconnected systems. The previous paragraphs illustrated that societies have become more dependent on cyberspace, and in particular networked systems such as the internet. Overall, losses from cybercrimes are remarkably higher in countries with a high level of internet penetration. Therefore, countries with a high number of internet users are expected to be more preoccupied with cybersecurity measures and hence are likely to give the issue more prominence and initiate counter measures (UNODC, 2013).

Countries are wary with regards to cyber vulnerabilities. According to Lewis (2002) the current situation in which countries are increasingly 'more dependent on computer networks' for the functioning of many aspects of their daily operations, including critical infrastructure, has created 'a massive electronic Achilles' heel'. These vulnerabilities can be exploited by individuals, groups and even by other nations. As a result, the increased usage of cyberspace has led to a new risk situation (Lewis, 2002, pp. 1). Both governments and their citizens are increasingly more dependent on the proper functioning of the networked computer systems. Therefore, countries with a high level of internet penetration are expected to be more concerned with cybersecurity when compared to other nations.

It only takes a single unaware of incautious user to grant access to malicious users. Consequently, as the number of internet users increases, the level of vulnerability increases. As Lewis (2002) puts it "these changes will lead to increased vulnerabilities if countries do not balance the move to become more networked and more dependent on Internet protocols with efforts to improve network security, make law enforcement more effective, and ensure that critical infrastructures are robust and resilient" (pp. 11). Hence, increased internet usage should be matched with increased cybersecurity measures. More and more users, and most of the literature inspiring fear, has led governments with large numbers of internet users to stimulate cyber defense mechanisms.

The increased cyber security awareness stemming from increased internet usage can be seen in China. Since 2007, "China has become a world leader in the communication industry", with over 500 million mobile phones and an internet population of more than 210 million people. This development has led the China government to increase cyber capabilities, both for internal unrest and outside threats. As the next paragraph will illustrate, China has made cyber capabilities a spearhead and aims to become a world leader in the area (Fritz, 2008).

Another option would be to focus on the number of internet exchange points or internet outlets rather than the internet penetration rate. However, this does not indicate the usage of the internet. The internet penetration entails the number of internet users per 100

inhabitants, which provides the actual usage. The internet exchange merely illustrate physical infrastructure. The internet exchange is often distributed to other data centers. Furthermore, this would allow only measuring the inbound and outbound traffic without providing information on individual usage. The argument here is that the more individual users, the higher the vulnerability, hence a higher need to have an effective set of cybersecurity policies. Therefore, the internet penetration rate is preferred as this indicates the actual individual usage (Xu, Duan, Zhang, & Chandrashekar, 2004).

2.4.3 Military expenditure

This section will use examples from both the public and the business sector, which is where most of the information and research on cybersecurity is available from, to illustrate the importance of military expenditure as a determinant for the cybersecurity policies of a country. Overall, the general trend appears to be that governments are significantly increasing their cybersecurity frameworks in order to counter possible attacks from unfriendly nations and malicious users of the internet.

The reason for choosing military expenditure as a determinant of a country's cybersecurity policies can be found in the fact that most countries consider the internet as a potential warfare tool. As Fritz (2008) mentions "the US has viewed the internet as a potential tool of warfare since its inception. Arpanet, a precursor of modern internet, was heavily funded by the US military".

Additionally, network-centric warfare (NCW), which started in the 1990s, has "become a core military branch along with the Army, Navy, Air Force, Intelligence, and Space" (pp. 40). The current situation of the US shows that this perspective has not altered much. The reliance of the United States on the internet as a security tool has not diminished since its start.

This situation is not unique for the United States. The previous paragraphs showed the continued investment in cybersecurity measures from countries such as the Netherlands and Denmark. Especially Denmark considers cyber defense a crucial part of their future military strategy and ranks it along with other vulnerable sectors such as the Arctic and has reserved significant amounts of funds to continue development in the cybersecurity sector (Danish Government, 2012).

Furthermore, non-western countries, such as China, have spent increasing amounts of money on increased cyber capabilities. China sees the cyber sector as one the main military

areas in which it can compete with other military strong countries and has made it a crucial area for continued development as it will take much longer to attain military competitiveness in conventional areas (Fritz, 2008).

As a company becomes more dependent on "reliable and secure computer processing and communications, the more the company needs to spend to assure the confidentiality, integrity, and availability of its sensitive information, intellectual property, and critical cyber processes and equipment" (Braithwaite, 2001, pp. 4). This is similar for governments, the more the country becomes dependent on cyberspace for its daily activities, and the more it needs to invest in protecting it.

For the realization that proper cybersecurity is necessary to arise often the issue must receive the attention of the company leaders, similar to the awareness stage discussed in chapter 2. Often, an issue receives attention when one of more attacks has occurred or other business leaders have issued it to be an important topic (Braithwaite, 2001).

A non-quantifiable argument, as Braithwaite (2001) puts it, is the notion that "is simply a cost of doing business in cyberspace", as it is in many other fields (pp. 4). One of the most prominent differences between the business and public sector is the fact that whereas companies suffer mostly potential revenue loss, governments run the risk of losing crucial personal and confidential information, disruptions of critical systems and other disruption to other non-quantifiable or non-economic governmental aspects.

Rather than focusing on how countries prepare against possible cyberattacks, a possibility would be to focus on the number of attacks a country encounters. This approach would reveal how countries respond to actual attacks and how these are influencing governmental policies. Nevertheless, as stated before, reliable data on the number of cyberattacks is not readily available.

This is the result of two main reasons; first of all, governments are reluctant to declassify this information as this can potentially expose vulnerable areas of their cyberspace. Secondly, most cyberattacks are not noticed or only noticed at a later stage which diminishes the active response mechanisms of a country (Bayuk, 2010). Therefore, the military expenditure of a country appear to be the most fruitful determinant at this point in time.

3. Method

In order to analyze which policies are currently in place, first of all, a framework – or test-scenario – will be developed, against which the countries under scrutiny can be analyzed. The idea behind this is to see why certain policies are chosen, and on which information or theories these policies are based. The dependent variable for the framework is the **level of development of a country's cybersecurity policies;** which policies are used and why did these develop into their current nature.

The quantitative analysis will use the Country Analysis Model, as discussed in chapter 3.2, to rank countries according to their attained level of cybersecurity policy development. In order to do this, the 23 countries' (cyber) policy documents will be examined out of which a detailed description, provided in appendix G, of the current situation becomes apparent. Furthermore, these country analyses are briefly summarized in chapter 4. Overall, the information from the policy documents is analyzed with the Country Analysis Model, which makes it possible to rank countries accordingly and hence forms the basis for the dependent variable.

For the quantitative analysis, three determinants will be used in an attempt to explain the attained policy development scores of the 23 individual countries. The determinants, as discussed in the previous chapter, are the internet penetration rates, military expenditure, and level of technological development. With the use of the a multiple linear regression, the data is analyzed to find the effect of each independent variable of the overall policy development score.

Cybersecurity in its broadest form is often described as "the absence of unauthorized intrusion into computer systems and their proper functioning" (Kello, 2013, pp.18). However, there is a problem with this general indictor; governments and companies are reluctant to admit an intrusion. Additionally, users are often unaware of the intrusions into their computer system which further undermines the reliability of the number of attacks they encounter. Therefore, the number of attacks will not be used as an indicator for this research.

According to Kellstedt and Whitten (2007, pp. 106-108) a measurement is reliable when the findings are consistent and repeatable. This indicator has a relatively high level or reliability, given that any researcher accessing the published numbers would find the same results. Nevertheless, this is not a conclusive indicator, given that is does not tell how many attacks have been prevented, furthermore, some countries or companies might be more high-profile, which would explain the higher number of attacks. Therefore, the design will be

somewhat different and will go beyond mere intrusions in a country's computer systems.

This chapter will start by explaining the unit of analysis. Following this, chapter 3.2 will introduce a policy development model which will help determine the level of development of maturity of a country's cybersecurity policies. Chapter 3.3 elaborates on the chosen explanatory factors or variables which will be computed with the use of an ordered logistical regression, as will be explained in chapter 3.4. The goal is to quantitatively analyze which factor influence the level of development of a country's cybersecurity policies. Finally, with the use of the quantitative data a case-study will provide the reader with a more comprehensive and practical example, the set-up of which will be discussed in chapter 3.5.

3.1 Unit of analysis

The individual unit of analysis used for this research is a country (Kellstedt & Whitten, 2007). The units of analysis for this research are 23 countries which have provided documents to the NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE). There is a difference with overall NATO Membership for the reason that Albania, Bulgaria, Croatia, Greece, Iceland, Luxembourg, Portugal, Romania , Slovenia and Sweden are excluded. These countries have been excluded because either their information is not included in the NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE) – indicating that their policies and documents are not up-to-standard – or because the necessary information is not published in either English or Dutch.

The CCDCOE database contains information on Austria, Australia, Finland and New Zealand and these countries are therefore added instead. Although these countries are not members of the NATO, they have been significantly developing their cybersecurity policies and are included in the data from the CCDCOE. The reason for choosing the NATO CCDCOE participants can be found in the fact that cybersecurity is a primary aim of the participants. Furthermore, all the included countries have either been involved in the drafting of, have signed, or ratified the Council of Europe's Convention on Cybercrime (from heron referred to as the Budapest Convention).

Another important feature of the countries under analysis is the fact that all have published national strategy papers which address cybersecurity as a primary concern or have published a Cyber Security Strategy paper. As discussed in chapter 2, security papers are important documents and show the commitment and awareness of countries towards specific security goals. Therefore, the country analyses will be primarily based upon the most recent

editions of either the National Security Policy of Cybersecurity Policy documents, depending on which have been published by the different countries. Finally, all the countries analyzed have

Given the above conditions, these countries can be assumed to value cybersecurity and the development thereof. Additionally, the NATO members are assumed to have similar military strategies as a result of their cooperation, and because no developing countries are a member we can assume that the countries have a relatively high level of technological development. Overall, the quantitative part of this research can be classified as a "large-N" design (Kellstedt & Whitten, 2007).

3.2 Determining policy maturity – the Country Analysis Model

To have a classification of the level of development a modified version of two National Institute of Standards and Technology (NIST) models will be used. The model – the Country Analysis Model – is a combination of the NIST Maturity Model and the 'NIST Framework for Improving Critical Infrastructure' (2014). The National Institute is an American Federal agency preoccupied with technological measurements, tests, and standards. The models use measurements "based on lessons learned and predictive indicators derived from previous and current cybersecurity activities (National Institute of Standards and Technology, 2014, pp. 11). This measurement is used for the Country Analysis Model as well; where indicators are based upon current and future policies and activities of the 23 countries in the area of cybersecurity.

Whereas both NIST models focuses specifically on corporations, for the scope of this article laws, regulations, reports and other official documents of governments will be used to determine the maturity of the policy. The reason for choosing the NIST models as a foundation is the fact that these are respectable and frequently used model for the determination of cybersecurity standards within companies (National Institute of Standards and Technology, 2014; Xiao-yan, Yu-qing, & Li-lei, 2011). Nevertheless, as stated above, the model are not sufficient and are complimented with findings and indicators specific for countries and based upon the literature review and theoretical framework.

The developed 'Country Analysis Model' uses the governance and risk assessment levels of the 2014 NIST framework and combines it with three of the maturity levels of the NIST Maturity Model. As the literature review and theoretical framework indicate, cybersecurity transcends borders, requires separate agencies – as cybersecurity is a new

domain – and a strong legal foundation to provide law enforcement agencies with adequate means. The NIST models alone are not fit to measure these three determinants which is the reason a new model has been developed for this research; taking into account the NIST models but primarily focusing on these three dimensions.

Countries differ from companies in as much as they cannot implement one security protocol and integrate this into their IT practices. Governments have many different agencies, departments and ministries and one integrated protocol cannot suffice to protect the cyberspace. Additionally, governments are exposed to and preoccupied with more and different types of cyber threats when compared to companies. Countries need to take into account a wide array of threats from cyberterrorism to cyberwarfare.

Therefore, the company based NIST models are not sufficient for this research. Overall, there are three main indicators used to determine the level development of a country's cybersecurity policies which the developed model takes into account; legal foundation, agency responsibility, and international cooperation. The policy findings of the 23 different will then have to be analyzed with the Country Analysis Model out of which an overall score can be determined per unit of analysis.

3.2.1 Legal foundation

The model has three dimensions; first of all, a legal foundation is crucial for an effective cybersecurity regime. Therefore, the number and scope of laws and regulations imposed for the protection of a country's cyberspace will be analyzed. The legal foundation articulated in cybersecurity policies of the countries and the findings under scrutiny will be ranked according to their level of maturity with a range from 1 to 3. With level 1 – policies – being the lowest and level 3 – integration – the highest level of development. The legal foundation dimension is concerned with whether or not "formal documented and updated policies are communicated to all employees" and if additional national documents or international agreements have been implemented (Xiao-yan, Yu-qing, & Li-lei, 2011).

The dimension further discusses if "legal and regulatory requirements regarding cybersecurity including privacy and civil liberties obligations, are understood and managed" (National Institute of Standards and Technology, 2014, pp. 21). As discussed in the previous chapter, the absence of legal documents does not necessarily indicate an absence of cybersecurity policies. Therefore, for the determination of the policies formal statements, speeches and reports will additionally have to be analyzed. On aggregate, these findings will

help to determine the development of a country's cybersecurity policies.

3.2.2 Agency responsibility

The second step is to examine which agency is responsible; if a separate cybersecurity agency or department is created or if different agencies cooperate within a government for the protection of cyberspace. An important aspect is to see what level of independence the agency responsible has and whether or not all aspects of cybersecurity are included or only some. Therefore, the second dimensions is concerned with the structure and the capabilities provided for the response to cyber incidents and threats and has three levels similar to that of the legal foundation dimension; where the first level 'policies' is the lowest and the third 'integration' the highest.

3.2.3 International cooperation

Finally, international cooperation, agreements and related documents are investigated. Most countries are highly aware of the fact that for a secure cyberspace cooperation is crucial. However, not all countries have the means of show the willingness to actively engage in partnership agreement. The final dimension will investigate the international participation of the different countries on a three-tier scale. The first level indicates a passive membership and limited engagement; if a country is at the second level it indicates that presence at international meetings is visible and some information sharing is done; the third level should be interpreted as strong international engagement and a country is actively putting the issue of cybersecurity on the international agenda.

3.2.4 Policy development score

The three different dimensions all have a three-tier scale. Level 1 indicates the limited progress of a country in that dimension and results into a 1 out 3 possible points; level 2 indications a country in an implementation stage and results into 2 out 3 possible points; level 3 indicates an integrated approach and results into 3 out 3 possible points. This grading scale will be done for all three dimensions.

In essence, a country can obtain a maximum of 9 out 9 points. For example, if country A is at level 3 on the 'legal dimension' scale, level 3 of the 'agency dimension' and level 2 in the 'international cooperation dimension', the country has a overall score of 8 out 9 possible

points. The analysis will be done for all 23 countries and result into a classification table which indicates the level of development of its cybersecurity policies.

The measurement reliability is relatively high, given that most governments have published an English strategy document on the CCDCOE website which summarizes the main legal documents, and different agencies and departments present in a country. Furthermore, laws and regulations can be found both on the internet and in law books.

However, the determination of laws and regulations in favor of cybersecurity are subject to some form of bias, given that the benefits for cybersecurity might not always be clear and disagreement is possible. The measurement validity is relatively high because it illustrates the developments present in the field of cybersecurity which is what this research focuses on (Kellstedt & Whitten, 2007).

Table 1: Country Analysis Model

Level of development / Analysis dimension	1. Policies	2. Implementation	3. Integration
Legal foundation	Country expresses willingness to cooperate with the current legal foundation Country aims to improve legal framework in the future	Country is reviewing legislation and making proposals for improvement Legal and regulatory requirements regarding cybersecurity including privacy and civil liberties obligations, are understood and managed	Legal framework is adjusted to include new international and domestic obligations which are already implemented Legal framework is continuously reviewed and when necessary adjusted Multilateral and bilateral agreements are actively supported
Agency responsibility	Risk responses are identified and prioritized Overarching structure exists but does not cover all security protocols Clear leadership or independent agency is absent	Overarching agency is planned or recently established Division of roles and actions is clear in all possible threat scenarios Authority is comprehensible and provided with capabilities and clear mandate	Adequate tests are routinely performed to ensure that all policies, procedures, and controls are acting as intended. Effective corrective actions, self-assessments, and independent audits are performed Policies, procedures, implementations, and tests are continually reviewed and improved. Continuous cost-benefit analysis is performed
International cooperation	Country is primarily a passive member in international forums Country expresses willingness to increase international cooperation	Threat and vulnerability information is received from information sharing forums and sources Country actively attends international meetings on a regular basis	Country is an active participant in international forums and is regarded as an important player in the field Country is forerunner and strives to persuade others to improve international cooperation

3.3 Independent variables

The variables used are: the level of military expenditure, the level of technological development of a country and the internet penetration (Kello, 2013; Kim, Wang, & Ullrich, 2012). These factors are expected to influence the level of development of a country's cybersecurity policy. Although more indicators can be thought of, these three are expected to be the most important. The scope and time limit of this thesis does not allow for investigation of all possible indictors. However, the following paragraphs will discuss and elaborate on the importance of these variables and the reason for choosing them. Appendix C shows the table which will be used to summarize the findings.

3.3.1 Technological development

First of all, the level of technological development of a country is expected to influence its level of cybersecurity development because a significant level of technical knowledge is necessary for this aim. Technologically advanced countries are more likely to be targets of cyberattacks. Additionally, these countries have more possibilities to increase their cybersecurity policies as a result of the necessary funds and knowledge required. An example of this indicator can be found from country experience. The United States is subject to the majority of attacks, whereas most attacks originate from Asia and Eastern Europe. One of the reasons the U.S. is most frequently targeted is the high level of digital data and intellectual property. The same trend is visible in the corporate sector, where technology companies are more often targeted when compared to other firms (FireEye, 2013).

Technological development is a rather abstract term. However, it significantly differs from general economic development. Although 'technology is a key factor in economic progress' the two are not identical. The aim of this thesis is to see if a focus on technological development is a determinant for cybersecurity policies improvement. For the ranking of the 23 different countries the technological development index of the Martin Prosperity Institute (2010) will be used (see appendix E). The institute is one of the leading think-tanks in the area of specific factors for economic development and prosperity. Furthermore, the index used multiple factors, whereas other indices often only measure one of two of these indicators.

The index measures three factors to establish technological development. First of all, "the financial resources devoted to research and development as a share of the total economic output". Secondly, "the share of human resources devoted to R&D, measured as the share of the total labor force made up of researchers. And finally, "patents granted per capita, the

conventional measure of innovation. If the first two measure critical inputs to the process of technology generation, the third is a measure of innovative output" (Florida et. al., 2011, pp. 4).

In the research 75 countries are ranked based upon the above three factors. Therefore, for measurement purposes the findings will be divided into 5 categories. Countries 1 to 15 are classified as 'high' and are the most technological developed countries in the world. The second category is classified as 'above average' and consists out of countries ranked 16th-30th. The third category is countries 31 to 45 and is grouped as 'average'. The fourth category entails country 46 to 60 and have a 'below average' level of technological development. Finally, countries 61 to 75 are considered to have a 'low' level of technological development.

3.3.2 Internet penetration

Secondly, the internet penetration data can be accessed with the use of the World Development Indicators Index of the World Bank, which are publically accessible and regularly updated. The relation between internet penetration, and hence internet usage, and the risks to cyberspace is relatively straightforward. Countries with a higher number of internet users are exposed to more risks simply because it only takes one user to open a corrupted file or other malicious data to gain hackers access to a computer system. Therefore, the higher the number of users, the higher the risk.

The expectation therefore is that governments are more likely to develop cybersecurity policies when the internet penetration in their country is high. The findings in Appendix C indicate the number if internet users per 100 inhabitants. The analysis will find out if a correlation between the number of internet users and the level of development of a country's cybersecurity policies exists.

3.3.3 Military expenditure

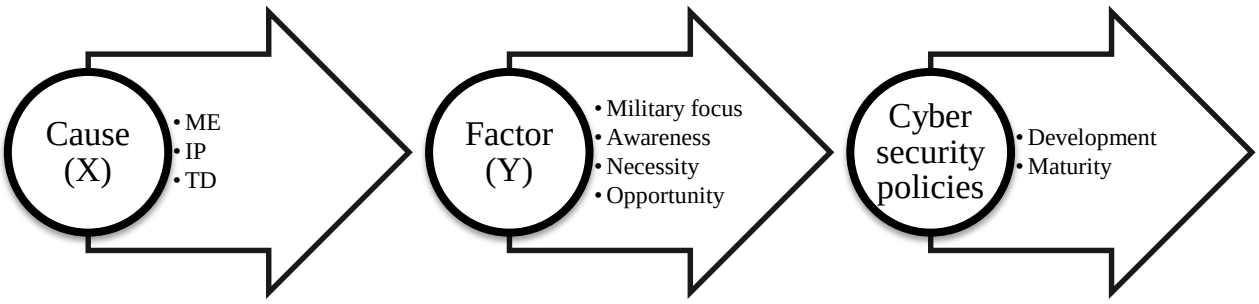
Finally, cybersecurity is frequently regarded in terms of conventional offensive and defensive military capability, as explained in chapter 2. In essence, the current knowledge on warfare dominates the perspective in which cybersecurity is held (Kello, 2013). Therefore, countries with a high level of military expenditure are expected to have a higher level of cybersecurity policy development as cybersecurity is some countries is part of their overall military strategy and considered as a fifth domain, next to air, land, sea and space operations. Therefore,

countries that traditionally have a high military expenditure such as the United States, Turkey, and the United Kingdom are expected to have a more developed cybersecurity framework.

The World Development Indicators (WDI), published by the World Bank Group, will be used as the measure of military expenditure. The WDI military expenditure numbers of 2012 are the most recent figures of the World Bank and hence these will be used for the analysis. The database of the World Bank has figures for all 23 countries and a considered to be a reliable source. The numbers are publically accessible, as explained in the previous paragraph, and therefore can be used by any researcher. Finally, the numbers used are denoted in terms of a county's GDP (see appendix C).

As figure 2 illustrates, three main determinants have been identified; Military Expenditure (ME), Internet Penetration (IP), and Technological Development (TD). The level of development of a country's cybersecurity policies is expected to be influenced by these three variables. First of all, a high level of military expenditure is expected to translate into a primary focus on military in general and hence the domain of cyberspace in particular. A high number of internet users is presumed to increase awareness of possible threats and a need to protect users. Finally, a specific level of technological development is required. Countries need to be in an opportunity to increase protection of their cyberspace. To increase cybersecurity policies a relatively high level of development and expertise is necessary. These independent variables will be used for in the analysis section.

Figure 2: Making cybersecurity policies



3.4 Multiple linear regression

Overall, the analysis will take into account the developments of the 23 different countries up until 2013, hence cross-sectional. Kellstedt and Whitten (2007) define cross-sectional as research in which "the time dimension is the same for all cases, and the dependent variable is measured for multiple spatial units" (pp. 27). The spatial unit for this research, as for many political science and international relations research, are countries. The time dimension is static; the analysis will the level of development the individual units had in 2013. Therefore, since the dependent variable, cybersecurity policy development, is measured for a constant time dimension the first part of this research fits the definition (Kellstedt & Whitten, 2007).

For the first step of the analysis, the articulations from the governments in the different countries will be analyzed. Following this, the implemented policies will be further investigated. This will be based upon the NCSS of the countries and attention will be paid to three main factors; which laws, regulations or other legal measures have been taken, which agencies are responsible and how are the task divided and cooperation stimulated, and which international treaties or agreements have been made. These three factors take into account the different dimensions discussed in chapter 2.1; governmental, national and international. These findings will be compared to the variables mentioned above; military expenditure, level of technological development and finally internet penetration (see Appendix C and I).

For the quantitative analysis a multiple linear regression will be used. The dependent variable, or outcome, is continuous. As chapter 3.2 indicates, the outcome for the different countries will be somewhere between 1 and 9, indicating the level of maturity of the cybersecurity policies, where 1 indicates a low level of maturity and 9 is considered to be the highest. The first independent variable, technological development, is ordinal. The other two explanatory factors, or covariates, are continuous and the aim is to find out which factors contribute to a higher level of cybersecurity policy development.

All independent variables are included, regardless of their significance. The variables are support with sufficient theoretical information and given that similar previous research is not present, all predictors need to be included; both significant and non-significant variables. Furthermore, no hierarchy exists between the independent variables and hence the forced entry method, rather than the hierarchical or stepwise methods is used in this study (Field, 2009, pp. 212).

The correlation between the explanatory factor for the unit of analysis, and the dependent variables will be examined. The equation for the multiple regression is: policy development

$score_i = b_0 + b_1$ technological development + b_2 internet penetration + b_3 military expenditure + ε_i. The policy development score is the outcome variable and *b* indicates the coefficients of the three predictors. Finally, ε_i indicates the difference between the predicted and the observed value of *Y* for the *i*th participant (Field, 2009, pp. 210). In essence, the level cybersecurity policy development is predicted based upon the level of technological development, internet penetration and military expenditure. When carrying out a multiple regression several assumptions need to be met; the types of variables used, multicollinearity, homoscedasticity, independence of errors, normal distribution, and linearity. If and to what extent these assumption are met will be provided in paragraph 5.1 before analyzing the findings.

3.4.1 Sample size

The multiple linear regression, as explained above, will be used to analyze 23 countries. The primary argument for not including more countries is the fact that the CCDCOE database only contains cybersecurity policy documents from 36 countries. Consequently, 13 countries are left out of the model. Out of these three countries did not provide documents in English or Dutch and hence are unable to be used due to linguistic limitations.

Furthermore, for Malaysia no recent information is available and the latest edition is from 2006. For Pakistan and Kenya no documents before 2014 had been published. Singapore has been left out as the document concerns the ‘2018 masterplan’ and hence no adequate analysis on the current situation is possible. Saudi Arabia only provided a consultation note, which is too limited in scope for inclusion into the model. The other five countries, India, Japan, South-Korea, Morocco, and Uganda are left out because they either did not participated or ratified the Budapest Convention or the document did not contain enough details.

In general, the sample is not in perfect accordance with some of the rules on multiple regression. Although there is no uniform agreement on the minimum size of a sample, 23 countries is at the lower end of the spectra and most authors would argue for the inclusion of more cases. For example, VanVoorhis and Morgan (2001) argue that there is not ultimate rule for the number of cases which are to be included in a research. However, they argue that “the general rule of thumb is no less than 50 participants for a correlation or regression” (pp. 140). This number increases as the number of independent variables increases. They use the formula of Harris (1985) which states that “the number of participants equals the number of predictor variables plus 50”.

The sample used in this research contains 23 countries (n = 23) and in total three independent variables are used. Therefore, according to the formula of Harris the assumption of sample size is not met. Other authors argue that 10 cases per independent variable can be sufficient, which in our case would entail 30 countries (Peduzzi, Concato, Kemper, Holford, & Feinstein, 1996). This number is significantly closer to our sample size, yet still larger.

Furthermore, Vittinghoff and McCulloch (2006) argue that 10 cases per independent variable is possibly a too conservative rule. The authors argued, based upon a large simulation study that "systematic discounting of results, in particular statistically significant associations, from any model with 5-9 EPV does not appear to be justified" (pp. 717). As a result of the study, they conclude that the rule of thumb of at least 10 predictor variables is not well-defined. Although the argument holds that including more cases can be beneficial for any model Nevertheless, if circumstances do not allow for this, the findings from a small sample can still be viable.

Moreover, most authors appear to agree on the fact that sample size is not the sole factor. Although "the more participants, the narrower the distribution, and the greater the likelihood that any differences will be discovered (i.e. the greater the power). Power is not, however, only related to sample size. Power is also related to effect size. The greater the effect size is, the greater the power" (pp. 140). VanVoorhis and Morgan further state that in situations where minimizing participants is critical "7 participants per cell, given at least three cells will yield power of approximately 50% when the effect size is .50" (pp. 139). Given the scope and time-span of this research, there is a need to minimize the number of participants. Furthermore, the participants were chosen based upon selected features discussed in chapter 3.1.

In a more recent edition VanVoorhis and Morgan (2007) further discuss the use of samples and some rules of thumb in which they acknowledge situations in which large samples sizes are inaccessible. The article states that "larger samples more accurately represent the characteristics of the populations from which they are derived. Consequently, larger sample sizes increase power and decrease estimation error. However, the practical realities of conducting research such as time, access to samples, and financial costs restrict the size of samples for most researchers" (VanVoorhis & Morgan, 2007, pp. 45-46).

In addition, using a smaller sample is not unique and even articles published in renowned journals have had small samples in the past. For example, Walter (1997) originally included 41 cases and decreased this number to 17 with 5 independent variables. Out of these variables, three were categorical with two containing more than 2 categories.

For example, the first hypothesis concerned outside security guarantees and options were coded as either ‘weak’; ‘moderate’; or ‘strong’.

Another example is the research of Scruggs (1999) which included only 17 cases and 7 independent variables. The argument put forward was that “the results are robust despite perennial small-n statistical problems encountered in comparative political economy” (pp. 1). Scruggs acknowledged the limitations due to the small *n* and achieved publication is the well renowned British Journal of Political Science.

Taking into account the above, a larger sample size would be preferable. However, this is not feasible for this research due to time restrictions and data availability. Future research is highly stimulated which would benefit from the inclusion of other independent variables and an increase of the sample size.

3.5 Case-study design

After conducting the quantitative research as “small N” research or case-study of a few cases will be carried out. Two countries will be intensively studied and compared. Whereas the first part is a statistical analysis, the case-study is helpful to gain some in-debt knowledge on two countries in specific (see appendix D). The units of analysis will be the Netherlands and Denmark. The reason for choosing these countries is the similarity in many aspects of the society and socio-economic development. Both countries have open economies, are highly technologically developed and have a high internet penetration. The table in appendix D shows that the Netherlands and Denmark both have 93 internet users per 100 inhabitants.

Additionally, the level of military expenditure is fairly similar. In 2012 the Netherlands spend around 1.3 percent of its GDP and Denmark 1.4 percent of its GDP on military expenditure (World Bank, 2013). Given this similarity in the independent variables these two countries are highly suitable for an in-depth comparison. Furthermore, as chapter 2.2 discusses, some differences in the level of development appear to be present between these countries. For a case-study it is important for the countries to have similar independent variables but differences in their dependent variable. This appears to be the case for the Netherlands and Denmark.

4. Country analyses

This chapter summarizes the findings of the countries and the obtained score for each of the three dimensions – legal foundation, agency responsibility, and international cooperation. The country analyses are crucial given that they indicate the level of development of the country's cybersecurity policy. Furthermore, the overall score will serve as the dependent variable for the quantitative analysis.

Before the analysis can be explained, it is important to recognize that international agreement on norms and standards is relatively limited. However, some improvement has been reached with the Council of Europe's Convention on Cybercrime (Budapest Convention). The Budapest Convention was effective as of 2004 and was the first big international Convention which lays down international judicial cooperation with regards to cybersecurity.

The parties to the Convention are required to transpose the provision into their national legislation. The Budapest Convention is a so-called 'open convention' and therefore non-member countries can accede to it, such as the United States and Canada. The Convention is widely regarded as the primary international foundation for cooperation – one of the key determinants for this research – and for that reason will be used as a condition. The 'openness of the Budapest Convention is also a weakness; countries are slow and reluctant to ratify the Convention.

The non-binding nature illustrates the reluctance of countries with regards to international standards and the struggle to respond to the constantly changing and developing nature of cyber capabilities. However, given the global incoherence in the terms used, as discussed in chapter 1.3, the Convention is the first attempt to bring countries on the same page and have some international agreement. All countries have either ratified or aided in the drafting of the Convention. Therefore, the legal foundation discussed in the next paragraph discusses additional steps taken by the countries (Council of Europe, 2014; Ministry of Defence Estonia, 2008).

4.1 Analyses summary

This paragraph will shortly summarize the findings of the country analyses. The more detailed description can be found in appendix G. Paragraph 4.1.1 will elaborate on the scores of the individual countries for the legal foundation dimension. Furthermore, the paragraph will highlight some commonalities between some countries as some will have the same scores.

Paragraph 4.1.2 is concerned with the agency responsibility and will indicate why the countries have received their respective scores. Following this, paragraph 4.1.3 discusses the international cooperation dimension. As the section will indicate some noteworthy differences are present between the different countries.

A general tendency is visible which hints at a more global perspective in countries such as Canada, Australia, the United Kingdom and the United States. These countries do not solely focus on Western countries but attempt to create partnerships with others as well. Whereas most continental European countries appear to foster more cooperation with regional organizations or Western organizations, such as the European Union, the OSCE, and the NATO.

Paragraph 4.1.4 uses the information of the previous chapters and will emphasize peculiarities and similarities within and between the countries. Finally, Chapter 4.2 will plot the implementation time of the Budapest convention with the individual policy development score. Overall, this chapter will investigate if there is a statistical significance between the time and the overall policy development score.

4.1.1 Legal foundation

The legal foundation of the different countries differs significantly. France, Lithuania, New Zealand, Poland, Slovakia and Turkey all are at level 1 – policies. These countries have either not ratified the Budapest Convention, such as Poland, New Zealand and Turkey – which will be discussed in further detail in paragraph 4.4, or have not succeeded in the implementation of new national legislation. The table in appendix I summarizes the main laws and regulations in the different countries. For example, Lithuania and Slovakia have ratified the Convention, yet have not taken considerable steps to improve cybersecurity legislation the domestic level.

The Budapest convention does not cover everything and should be considered as a first step to increase international information sharing and cooperation (Council of Europe, 2014). Lithuania’s national legislation is highly fragmented and the scope is rather limited. The Lithuanian cyber strategy expresses the awareness of the government for this dimension. National legislation should be improved and more clearly define roles and responsibilities (Government of the Republic of Lithuania, 2011).

Slovakia, is well on its way to properly implemented international norms and standards, such as those stated in EU directives, OECD recommendations and the Budapest Convention. Nevertheless, national regulations and legislation should be focused on country

specific risks and areas in addition. The Slovak government is at the policy level given that a national assessment is absent and no reforms have been introduced (Government of the Slovak Republic, 2008).

New Zealand is another peculiar case, the government has not implement the Budapest Convention and has not proposed any significant national legal reforms. The strategy paper only reveals an attempt to improve the legal framework and states that the country is considering international conventions (New Zealand Government, 2011). Lithuania, Slovakia and New Zealand are at the policy level for all three dimensions. What this indicates is a limited policy development and puts these countries at the bottom of the group.

Table 2: Legal foundation

Country	Legal foundation
France, Lithuania, New Zealand, Slovakia, Turkey, Poland	Level 1 - Policies
Austria, Belgium, Canada, Denmark, Finland, Germany, Italy, Latvia, Netherlands, Norway, Spain, Czech Republic	Level 2 - Implementation
Estonia, Hungary, United Kingdom, Australia, United States	Level 3 - integration

The majority of the countries are at the implementation stage – level 2. Most countries have incorporated international agreements and recommendations into their national legislation and have taken additional steps for their country-specific needs and situations. In general two main trends are visible within this category. First of all, Austria, Denmark and Finland are not in favor of a strict legal framework. All countries have introduced some legal reforms but are not actively pursuing new reforms and are not expected to propose new legislation in the short-run.

The other category, which includes Belgium, Canada, Latvia, the Netherlands, Italy, Norway, and the Czech Republic are currently in a process of additional reforms. Some progress has been made and these countries are making proposal for improvement. Therefore, these countries comprise the more active group whereas the others are more passive and are less preoccupied with further reforms and short-term reforms. Nevertheless, all the countries with a level 2 score have ‘understood and managed legal and regulatory requirements regarding cybersecurity and civil liberties obligations’ which explains their classification.

The Czech Republic has drafted an Act on Cybersecurity (2014), this act is an important step for the improvement of the Czech Republic’s national legal framework.

However, the Act is not implemented yet, and hence the Czech Republic is still at the implementation level. The Act should be examined in conjunction with the 'specialized law' of the National Security Authority. In addition, the Czech Republic has incorporated international recommendation and norms and standards such as those of the Budapest Convention, the EU and NATO (Strategy of the Czech Republic in the field of cybernetic security for 2012-2015).

Estonia is an exceptional case, the country has an overall score similar to that of the United Kingdom , with both countries scoring 8 out 9 possible points. The Balkan state thus scores higher than the highly developed Northern and Western European countries. The Estonian government is very active in legal reforms and reviews with new legislation, amendments and initiatives being launched ever since 2008. Hungary can be considered to be at the integration stage as a result of the swift implementation of the Budapest Convention and the highly detailed 2013 Act on Electronic Information Security of Central and Local Government Agencies. The Act takes into account the national actors, reactionary measures and the potential risk areas and threats (Government of Hungary, 2013).

The United Kingdom goes beyond its national legislation and regards it as an obligation to aid other countries to develop a proper legal basis for the area of cybersecurity. Furthermore, the British government is constantly taking new trends into account and hence reviewing existing legislation (Cabinet Office United Kingdom, 2011). Australia also receives 3 points, given its continuous development. The Australian government has implemented several legal reforms and is currently still active in the review of its national legislation (Australian Government Department of Defence, 2013). Finally, the United States arguable has the most developed legal framework. The country is both nationally and internationally active and has issued a significant amount of reforms to combat cyber crimes and terrorism.

Estonia, Hungary, the United Kingdom, Australia and the United States, are the countries which score highest on the legal foundation dimension compared to the other 19 countries. These four countries have taken significant national steps to improve their legal framework for the area of cybersecurity. Additionally, these countries are aware of the changing situation and are actively reviewing their national legislation. These countries can be classified as level 3 units given their integration of both national needs and international norms and standards into their legislation.

4.1.2 Agency responsibility

Belgium, Hungary, Italy, Lithuania, New Zealand, Slovakia and Spain are at the policy level and score a 1 out of the possible 3 points. Belgium has established a Centre for Cyber Security (CCSB) and a discussion platform known BelNIS. However, the different departments and agencies operate autonomously and are not given a clear mandate or resources (Belgian Cyber Security Strategy paper, 2012).

Hungary is still developing its organizational set-up, with excellence centers being an aim. The different organizations within Hungary are all individually responsible for their respective area and the coordination appears less developed. Furthermore, the Government Incident Centre, is only recently established and the cooperation with the Sectoral Incident Centers cannot clearly be established yet.

For agency responsibility Lithuania is again at the lowest level. Although CERT Lithuania is operational, no legislative reforms have been introduced to make it mandatory to report cyber incident to the CERT. At the moment, the Internet Traffic Exchange node is the only responsible agency, which is something the Lithuanian government is trying to improve (Government of the Republic of Lithuania, 2011).

New Zealand has been improving its organizational structure for cyber protection. For example, the 'National Cyber Security Centre' has been established. Nevertheless, the Centre, which falls under the Communications Security Bureau is to absorb the Centre for Critical Infrastructure Protection. Additionally, CERT New Zealand is under examination and the government is reviewing if renewal is necessary. Therefore, progress is being made but New Zealand is still at the policy level (New Zealand Government, 2011).

Slovakia is currently reforming its three-tier structure to improve the effectiveness and efficiency of the agencies responsible. The Slovakian government aims to create a National Information Security Authority to absorb the different bodies currently responsible and to have a clear authority (Government of the Slovak Republic, 2008). Spain has many different separate responsible organizations and agencies. However, an overarching structure is limited and clear leadership and authority somewhat absent. Spain would benefit greatly from one main responsible organization which would absorb all the different agencies.

The countries which are at level 2 for the agency responsibility dimension all have established or are currently implementing a central agency or authority which is responsible for coordination with regards to cyber incidents and the response to other cyberspace breaches. Furthermore, these countries have functioning Computer Emergency Response

Teams. Australia for example has established the 'Australian Cyber Security Centre', which takes up responsibilities previously divided between different agencies and CERT Australia will serve as the hub between the public and private sector. This is similar for all the countries at this level (Australian Government Department of Defence, 2013).

Table 3: Agency responsibility

Country	Agency responsibility
Belgium, Hungary, Italy, Lithuania, New Zealand, Slovakia, Spain	Level 1 - Policies
Australia, Austria, Canada, Czech Republic, Denmark, Estonia, Finland, France, Latvia, Netherlands, Norway, Turkey, United Kingdom	Level 2 - Implementation
Germany, Poland, United States	Level 3 - integration

Germany, Poland and the United States have the most clearly defined and elaborate organizational structure. The structures are clear in all three countries; indicating that the actors and relevant stakeholders are clearly defined, their roles and positions explicit and an overarching authority are established.

Furthermore, these governments have routinely performed tests to ensure the coherence of the procedures, controls and policies. These include corrective mechanisms and self-assessments. For example, the German government has called these 'effective analyses', which are similar to the scheduled risk assessments reports of the Polish government.

Finally, the countries perform a cost-benefit analysis on a continuous basis, thereby taking into account the fact that unhackable software is an unattainable goal and efficient responses are necessary (Federal Ministry of Interior Germany, 2011; Government of the Republic of Poland, 2013).

4.1.3 International cooperation

Latvia, Lithuania, New Zealand, Slovakia, and Turkey all have a limited development with regards to international cooperation. These countries score only 1 out of 3 points. The primary reason for this is the fact that these countries have acted more as bystanders rather than active participants at international forums. All countries have expressed the awareness and need to increase international cooperation and hence can be expected to increase their level of development for this dimension in the future.

The majority of the countries are at the implementation level. Most countries actively

participate at international forums and have to differing extents used the information sharing opportunities provided by the international organizations and meetings. The level 3 countries, Canada, Estonia, United Kingdom and the United States have a broader scope for international cooperation. The United States, for example, includes non-western international organizations such as Asian-Pacific Economic Cooperation (APEC). Given that cybersecurity is not a regional or local issue it is important to foster international cooperation. Therefore, active cooperation with African and Asian countries is crucial.

Table 4: International cooperation

Country	International cooperation
Latvia, Lithuania, New Zealand, Slovakia, Turkey	Level 1 - Policies
Australia, Austria, Belgium, Czech Republic, Denmark, Finland, France, Germany, Hungary, Italy, Netherlands, Norway, Poland, Spain	Level 2 - Implementation
Canada, Estonia, United Kingdom, United States	Level 3 - Integration

Furthermore, Canada, the United Kingdom, Estonia, and the United States are seen as important player in the field of cybersecurity. The United Kingdom and the United States have made it part of their respective policies to include and aid other countries (Cabinet Office United Kingdom, 2011). Estonia, partly as a result of the establishment of the CCDOE, is an important international actor which promotes information and technology sharing between all relevant stakeholders.

4.1.4 Commonalities and differences

Table 5, provided below, illustrates that Lithuania, New Zealand and Slovakia are at the policy level for all three dimensions. These countries all have published strategy documents in which they outline the plans for the future, however, they are not at the implementation level yet. Lithuania can be regarded as the country with the slowest progress. Although the Lithuanian government expresses an aim and need for continued development and future progress, it also indicates the relatively low development the country has in the area of cybersecurity right now.

Slovakia is somewhat further in as much as that a structure is outlined, something which is lacking in Lithuania, nevertheless the plans are currently still being developed and

proposing reforms. Therefore, Slovakia is not implementing anything at the moment. New Zealand can be regarded as the country which is closest to implementation. Although the cyber policy development of New Zealand is still in its infancy, some improvements are underway. The 'New Zealand National Cyber Security Centre' is an important step forward. Nevertheless, New Zealand is currently still mostly reviewing the existing structure and very little tangible developments have been accomplished.

Spain, Italy and Belgium are in a different situation than the Nordic block mentioned above. These countries are at the implementation level for their legal foundation and international cooperation. However, the countries are still introducing the appropriate structures and responsibilities, required for the agency responsibility dimension.

Table 5: Total scores

Country	Legal	Agency	International	Total
Lithuania, New Zealand, Slovakia	1	1	1	3
Turkey	1	2	1	4
Latvia	2	2	1	5
France	1	2	2	5
Belgium, Italy, Spain	2	1	2	5
Austria, Denmark, Finland, Netherlands, Norway, Czech Republic	2	2	2	6
Poland	1	3	2	6
Hungary	3	1	2	6
Germany	2	3	2	7
Canada	2	2	3	7
Australia	3	2	2	7
Estonia, United Kingdom	3	2	3	8
United States	3	3	3	9

Austria, Denmark, Finland, the Netherlands and Norway are also grouped together in the table below. These five countries are at the implementation level for all three dimensions. What this indicates is that the countries have published elaborate and comprehensive policies, which are not quite integrated yet. A praiseworthy feature is the fact that these countries appear to take a systematic approach in with regards to cybersecurity. The countries are developing the three dimensions at the same time and take a step-by-step approach to make sure every sector and issue is properly included.

Poland and Hungary on the contrary, have a more dispersed development. Although all countries have an overall score of 6, the differences in development are remarkable. Poland

has emphasized agency responsibility and hence developed a clear structure and assessment and risk analysis mechanisms, whereas Hungary has developed a strong legal framework for cybersecurity. This is the opposite of Poland which is currently still at the policy level for legal foundation and Hungary is at the policy level for agency responsibility. These countries have taken the opposite approach, with Poland first developing its internal structure and Hungary first securing a strong legal foundation.

It is important that not every situation or framework is appropriate for every country. Countries must determine and establish a system and structure suitable to their needs and demands. The analyses are based upon the information provided by the governments, primarily in their latest strategy papers. The analyses are an overview of the current situation, however, given that the area of cybersecurity is rapidly gaining in importance changes in the near future are likely. All governments examined are aware of the necessity of a strong and proper functioning set of cybersecurity policies.

There is no mold in which the policies should be casted. However, three main areas are important; legal foundation, to ensure a strong and comprehensive legal framework in support of the cyber policies; an clear structure and overarching authority to ensure the proper functioning of the different agencies; and international cooperation, as cyberspace transcends borders this issue is ever more pressing. The offensive and defensive capabilities a country has can differ significantly. For example, Lithuania cannot be expected to have the same capabilities as the United States. Nevertheless, the analyses do not take into account these capabilities, rather, it examines the overall structure and set of policies bases upon the above mentioned three dimensions.

Moreover, the differences between, for example, Turkey and Estonia are a result of effort and not military of economic strength. The Turkish army is far greater than that of Estonia, nevertheless, cybersecurity is a new dimension, different from conventional areas and hence new structures and procedures are necessary. Estonia has been subject to a large scale attack, as discussed above, and hence the prominence of cybersecurity was expected.

4.2 Significance of the Budapest Convention

The 23 countries all appear committed to improve their cybersecurity framework. As stated above the countries under scrutiny are affiliated with the NATO Cooperative Cyber Defense Centre of Excellence. Furthermore, all countries except Poland, New Zealand, Turkey and Canada have officially ratified the Budapest Convention (see appendix I for an overview).

The Budapest Convention stimulates international information exchange and defines which agency is responsible for correspondence. Furthermore, as stated above, the Budapest Convention is the most prominent international convention with regards to cyber crimes in existence today. Therefore, the importance of the Budapest Convention can be found in the prominence given to the topic of the parties to it. Furthermore, the ratification of the Budapest Convention hints at the necessary awareness as discussed in chapter 2.

The Convention addresses the three main dimensions, legal foundation, agency responsibility and international cooperation (Council of Europe, 2011). Nevertheless, the implementation of the Convention turned out to be a time-consuming process. The Czech Republic, Austria, Belgium, and Australia have only ratified the convention in 2012, despite the fact that Belgium and Austria were amongst the first signatory states in 2001 and the Czech Republic had signed the Convention in 2005. Australia has not signed the Convention in an early stage but decided to ratify it nevertheless in 2012.

This slow progress is visible in most countries, for example, Germany and the United Kingdom signed the Convention in 2001, but only ratified the agreement in 2009 and 2011 respectively. Lithuania, Estonia, Hungary, Denmark and Slovakia were the only countries to ratify the Convention within 3 year or less of signing the agreement. The ratification of the Budapest convention and hence the prominence of cybersecurity varies significantly amongst the 23 different countries. When plotting the numbers in SPSS figure 1 appears.

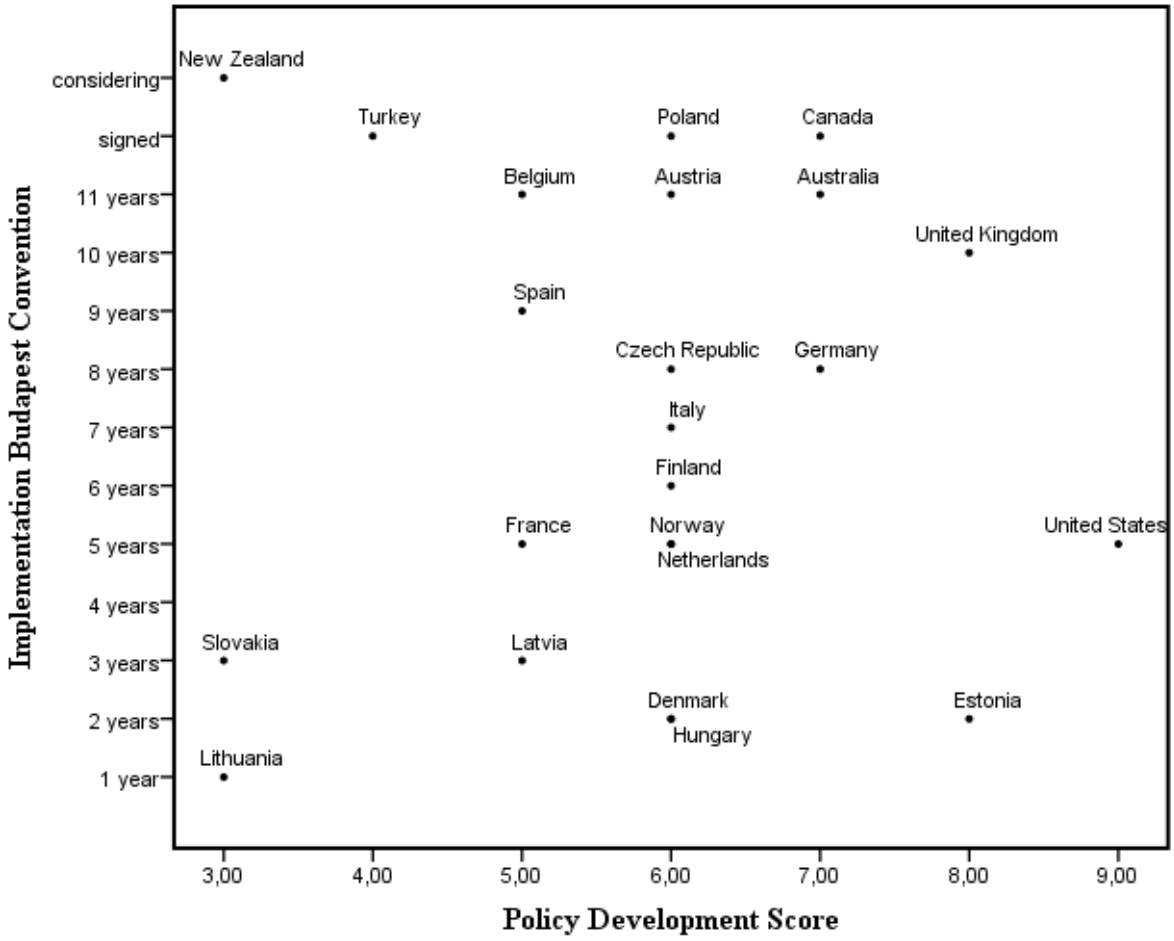
The years displayed on the y-axis in figure 1 indicate the amount of time a country took to ratify the agreement. For example, the United States took around five years to implement the Convention. New Zealand on the other hand has not signed the agreement and is merely considering becoming a party to it. Poland, Turkey and Canada have signed the convention yet not ratified it and are therefore to be found at the ‘signed’ level. The x-axis shows the attained policy development score of the 23 countries.

Overall, the implementation time of the Budapest Convention does not appear to influence the policy development score and is therefore not included in the statistical analysis of chapter 5. Although some countries confirm the expectations – a long implementation process results into a lower policy development score and vice versa – this is not the case for all countries. The biggest group, for example, which entails Denmark, Norway, Hungary, the Netherlands, Finland, Poland, Italy, Austria, and the Czech Republic, differs significantly. Although all these countries have a policy development score of 6 out of 9, the implementation time is highly different. As shown in figure 1, whereas Hungary and Denmark

implemented the Budapest Convention 2 years after signing, Austria needed 11 years and Poland has neglected to implement the Convention completely.

The duration of the ratification process of the Budapest Convention does not appear to strongly correlate to the level of policy development. For example, Slovakia and Lithuania, ratified the agreement in 3 and 1 year respectively. Nevertheless, these countries have the lowest policy development score. On the other hand, New Zealand and Turkey, have a very low policy development score and a have not ratified the Convention yet. The contrary is visible as well, whereas the United Kingdom and Canada have a high policy development score, the ratification process is lengthy in addition. Estonia and the United states are the only countries with a short ratification process and a high policy development score. Therefore, the expectations are not met and hence the influence of the implementation time of the Budapest Convention is not significant for the policy development score.

Figure 3: Implementation Budapest Convention



5. Interpretation of the data

The separate analyses of the 23 sample countries provide a clear overview of the development within the three different dimensions. Appendix G provides a table in which the scores per dimension and the overall score are given per country. When computing this data in SPSS no significant correlation appears to be present between technological development and the level of cybersecurity policy development (see table 7).

A link between military expenditure and the obtained score in the Policy Development Model appears to exist which will be further discussed below. Paragraph 5.1 examines whether and to what extent the necessary assumptions are met. Following this, paragraph 5.2 will use Cronbach's Alpha to evaluate the scale reliability of the country development model. Paragraph 5.3 analyzes the connection between technological development and the level of development of the units of analysis. Paragraph 5.4 and 5.5 are concerned with the internet penetration rates and military expenditure in relation to the overall policy development levels. Finally, some limitations of the quantitative design will be discussed in paragraph 5.6

5.1 Assumptions

A regression analysis on a sample requires that several assumptions are met. Therefore, this paragraph will discuss the types of variables used, outliers, multicollinearity, homoscedasticity, independence of errors, normal distribution, and linearity. The primary aim is to explain assumptions and to what extent they are met.

5.1.1 Variable types

For a multivariate logistical regression all independent variables must be quantitative or categorical with two categories. However, technological development is categorical, running from high to low development on a five point scale. For strict interpretation of a multiple regression model does not permit the use of a categorical variable when it contains more than two levels. The most common option would be to use dummies to work around this flaw (Field, 2009). However, given that the quantitative analysis is a small *n* study, with 23 cases in total, the inclusion of dummies is not feasible. The reason for using the categorical variable stems from the fact that a ranking from the Martin Prosperity Institute is used.

The raw data is not readily available and hence the actual numbers of technological development cannot be used. Actual numbers would require additional in-depth investigation which is not the aim of this research. Neither the time nor scope would allow for this. The

reason for using technological development, as further explained in chapter 3.3.1, is the fact that for cybersecurity policy development the actual technological development information is deemed necessary rather than overall economic development or the size of a country's services sector relative to the production sector. Furthermore, there must be non-zero variance. In essence this means that the predictors or independent variables should have variations in value. This assumption is met given that all the values between and within the predictors differ for all cases.

5.1.2 Outliers and influential cases

Appendix J summarizes the case summaries. From this information we can state that no case has a greater Cook's distance than 1. To put it differently, none of the cases has an excessive or unjustified influence on the overall model. Furthermore, the table provides the centered leverage values. The average leverage value is 0.17 ($k + 1/n = 4/23$). Values which are twice (0.34) or three (0.51) times as large can indicate influential cases. Case 23, the United States, is slightly above the boundary of three times the average with a value of 0.58. Turkey, case 21, has a value above twice the average leverage, with a value of 0.42.

There is some debate about which rule to follow. However, for now, the United States is the only case which might require further attention. All other cases, according to the evidence presented, are not unduly influencing the data. To further find influential cases, the standardized DFBeta can be used. As is visible in the table in Appendix L, no case has an absolute value greater than 1 and hence the cases are acceptable. Again, some debate exists as to where to put the cut-off point. For example, Stevens (2002) argues that 'cases with absolute values greater than 2' should form the cut-off point. Nevertheless, as all cases in this research are below 1, the debate does not affect our findings.

Finally, the covariance ratio can be used to find influential cases. The values should fall between $1 + [3(k + 1)/n]$ and $1 - [3(k + 1)/n]$. For the cases in this thesis this entails that the values should fall between 1.52 (1 + [4*3/23]) and 0.48 (1 – [4*3/23]). Case 12 (1.70), case 20 (1.58) and case 21 (1.84) are slightly above the upper bound and are not expected to have undue influence. The problematic case is the United States, case 23, which stands out with a value of 3.30. Nevertheless, according to Field (2009) if the Cook's distance is acceptable 'there is probably little cause for alarm'. Given that the Cook's distance for case 23 is 0.0428, the United States is kept in the dataset.

5.1.3 Multicollinearity

The multicollinearity assumption requires that there should not be an "a perfect linear relationship between two or more of the predictors" (Field, 2009, pp. 220). A problem with collinearity is present when the tolerance value is less than 0.1. For all independent variables the tolerance value is higher than 0.1. The values are 0.513 for "technological development"; 0.517 for "internet penetration"; and 0.933 for "military expenditure". Furthermore, the variance inflation factors (VIF) should not have a 'value greater than 10'.

The VIF values are 1.949 for "technological development"; 1.933 for "internet penetration"; and 1.072 for "military expenditure". Therefore, all values fall within the allowed range and neither the tolerance nor the VIF values indicate a problem with collinearity. Finally, when the 'average VIF is substantially greater than 1' there might be reason for concern. The average VIF value for our model is 1.65 (1.949+1.933+1.072/3) and is deemed acceptable as it does not substantially differ from 1 (Field, 2009, pp. 224).

For collinearity the eigenvalues and the condition indexes in appendix K can be a helpful tool to point out problems. The eigenvalues should not have great differences between them as this might make the model susceptible to 'small changes in the measures variables'. Furthermore, if one condition index is far greater than the others this might indicate a problem with collinearity as well.

The final dimension has a condition index of 29.98, which is higher than all others. Despite the fact that there are not strict rules 'about how much larger a condition index needs to be to indicate collinearity problems', some further investigation appears to be necessary. The table also indicates the variance proportions and a problem might be apparent when predictors 'have high proportions on the same small eigenvalue'.

For the final dimension, both technological development and internet penetration have high proportions. Statistically speaking, there is no 'grounds for omitting one variable over another'. Given that the proportions are not excessive, the variables will both remain included in the model. For future research including more cases might lessen the proportions (Bowerman & O'Connell, 1990).

5.1.4 Homoscedasticity

For the first step to determine homoscedasticity the graph in Appendix J will be used. As Field (2009) states "if this graph funnels out, then the chances are that there is heteroscedasticity in the data. If there is any sort of curve in this graph then the chances are

that the data have broken the assumption of linearity" (pp. 247). The points in the graph appear to be relatively random and even dispersed. This hints at both linearity and homoscedasticity and hence to meet the assumptions.

Overall, this assumption of homoscedasticity is met when "the residuals at each level of the predictor(s) have similar variances" (Field, 2009, pp. 787). Appendix K displays the residual statistics table in which it becomes apparent that none of the cases has a standardized residual less than -2 or greater than 2 and hence this assumption is met.

5.1.5 Independence of errors

Another assumption concerns independent errors and the Durbin-Watson test is a frequently used method. In essence, "for any two observations the residual terms should be uncorrelated. The "test statistic can vary between 0 and 4 with a value of 2 meaning that the residuals are uncorrelated" (Field, 2009, pp. 785). For our model the Durbin-Watson value is 2.208 and hence close to 2 indicating a high likelihood of uncorrelated residual terms. As a result, the assumption appears to been adhered to.

5.1.6 Normal distribution

To determine normal distribution the distribution of residuals is used. According to Field (2009) "it is assumed that the residuals in the model are random, normally distributed variables with a mean of 0 and a standard deviation of 1" (pp. 102). What this entails is that "the differences between the model and the observed data are most frequently zero or very close to zero, and that differences much greater than zero happen only occasionally (Field, 2009, pp. 221).

The histogram in appendix M illustrates the distribution of the standardized residuals. No high kurtosis is visible, neither as a negatively or positively skewed distribution. The histogram displays a normal bell-shaped distribution. For further examination of the residuals the standardized residuals are entered into a scatter plot. The scatter plot in appendix M illustrates the dependent variable in a normal P-P plot of the regression standardized residuals. In the scatter plot the observed cumulative residuals are plotted against the expected cumulative residuals. As can be seen, the residuals are normally distributed given that the points are roughly situated on the straight line and the assumption is met.

5.1.7 Linearity

For the linearity assumption to be met the "values of the outcome variable for each increment of the predictor(s) must lie along a straight line" (Field, 2009, pp. 221). The scatter plot in appendix J of the standardized residual can be used for this. The figure displays no clear pattern and the residuals appear to be dispersed around the reference line. As stated in paragraph 5.1.4, the model appears to meet the criteria of linearity.

5.2 Scale reliability

According to Field (2009) Cronbach's Alpha is the 'most common measure of scale reliability'. The country development scale was developed for this research and hence the reliability has not previously been tested. Therefore, Cronbach's Alpha will help determine the reliability of the country development scale. Generally a value of .7 to .8 is acceptable. The value for Cronbach's Alpha should not be lower than .7, any value lower than this indicates 'an unreliable scale' (Field, 2009).

The tables in appendix N illustrate that Cronbach's Alpha is calculated as the reliability statistic. The Policy Development Model was found to be reliable (3 items; α = .71). The means and standard deviations are reported in Appendix O and P; Legal foundation (M = 1.96, SD = 0.71), agency responsibility (M = 1.87, SD = 0.63), and international cooperation (M = 1.96, SD = 0.64). The sample size for each subscale was 23. What these numbers indicate is the fact that most countries attained a little under 2 out of 3 points on each of the subscales. The average score for the legal foundation and international cooperation dimension is 1.96, and for the agency responsibility dimension is 1.87.

Furthermore, the three different items should correlate with the total and hence be above .3. The third table in appendix N provides the Corrected Item-Total Correlation: legal foundation = .530; agency responsibility = .336; international cooperation = .749. Given that all three items have a total higher than .3 indicates that none will have to be deleted and all correlate with the total.

A problem with the measurement is the error which can occur when a scale includes a large number of items. The larger the number of items, the more the outcome of Cronbach's Alpha will increase without the reliability necessarily becoming higher (Cortina, 1993). However, the number of items on the country development scale is rather small; only 3 items are included – legal foundation, agency responsibility, and international cooperation. Therefore, this problem is not present and hence the Alpha is expected to be reliable.

The only problem encountered concerns the individual scores of the international cooperation and agency responsibility dimension. The third table in appendix N illustrates the overall alpha if this item is deleted, which would be .32. The value of Cronbach's Alpha = .71 and all values should approximately be the same. However, international cooperation would properly alter the overall number. On the contrary, excluding agency responsibility from the scale would increase the Alpha to .82 and hence improve the score. Nevertheless, given that the scale only consists out of these three items, and that the dimension are sufficiently supported with the literature presented above, no item will be deleted.

Overall, Cronbach's Alpha for the three different dimensions of the Policy Development Model is .71 ($\alpha = .71$) and hence can be regarded as acceptable. Furthermore, the Item-Total Correlation for all items is sufficient. Some minor problems appear to be present with regards to individual importance of the items. International cooperation and legal foundation appear to be more positively influential when compared to agency responsibility for the total Alpha. Thus, internal consistency of the scale is established. The following paragraphs will discuss each of the independent variables and the results out of the linear regression data from SPSS.

5.3Internet penetration

This paragraph will analyze relation between the level of cybersecurity policy development – the dependent variable – and the internet penetration and military expenditure levels of a country. The findings presented in chapter 5.5 will illustrate that technological development is not significant for the level of cybersecurity policy development. The results distorted the findings and hence the variable is excluded from the model in the following to paragraphs and hence with the use of bivariate analyses the significance of internet penetration and military expenditure on the level of cybersecurity policy development will be examined.

Table 6 and the first table in appendix O, reveal a significant correlation between the dependent variable and the independent variables; $R = .62$. Furthermore the R^2 value = .38, which indicates that 38% of the changes in the level of policy development can be explained by the independent variables. The adjusted R^2 is inherently lower as it accounts for other possible indicators, as explained above. Overall, taken the adjusted R^2 into account, 31.8% of the variation in the level of policy development can be explained with the use of the model.

Table 6: regression analysis - coefficients (excluding TD)

	B^*	$SE\ B^*$	β^{**}	t	p
Constant	.76	1.98		.38	.706
Internet Penetration	.041	.023	.313	1.77	.092
Military Expenditure	1.16	.37	.56	3.16	.005

Note: R^2 = .38, Adjusted R^2 = .32, * Unstandardized coefficient, ** Standardized coefficient, total $p < .008$

Appendix O further indicates the analysis of variance. MS_M is 10.25 and large in comparison to the $MS_{R;}$ indicating that the model as a whole improves the prediction. Both the *F*-ratio and the MS_M are in this model larger compared to the model including technological development. Overall, the chance that an *F*-ratio of 6.14 occurs if the null hypothesis is correct is .9 percent; $F = 6.14$ which is significant at $p < .009$. Furthermore, table 11 indicates an overall significance of .008 and hence as one is statistically significant, in essence different to 0.

Moreover, table 6 illustrates that $b_0 = 0.758$, and hence the model predicts a policy development score of .76 if *X* is 0. Additionally, b_1 internet penetration is 0.041 with a significance of .092. Therefore, a problem is present with regards to the internet penetration dimension. Although the indicator appears to be more significant when compared to the previous model ($p = .092$), the indicator is only statistically significant if $p < .05$ (Field, 2009). As a result, internet penetration does not appear to be a good indicator for the level of cybersecurity policy development.

As the indicator table in appendix C shows, the numbers vary significantly from country to country. Overall, the Northern European countries, such as the Netherlands, Denmark, Finland, and Norway all have an internet penetration above 90 users per 100 inhabitants, whereas, Turkey, Lithuania, Poland and Italy have an internet penetration below 70. A first glance, a small relation appears visible.

The Netherlands, Denmark, Finland, and Norway all have a score of 6 out of 9. On the other hand, Turkey and Lithuania scores a 4 and 3 respectively. However, Italy and Poland both have a score of 6 – similar to that of the high internet penetration countries. Furthermore, New Zealand with an internet penetration of 89,5 and Slovakia with 80 per 100 inhabitants, are both still completely at the ‘policies’ level and have a score of 3. Consequently, no strong

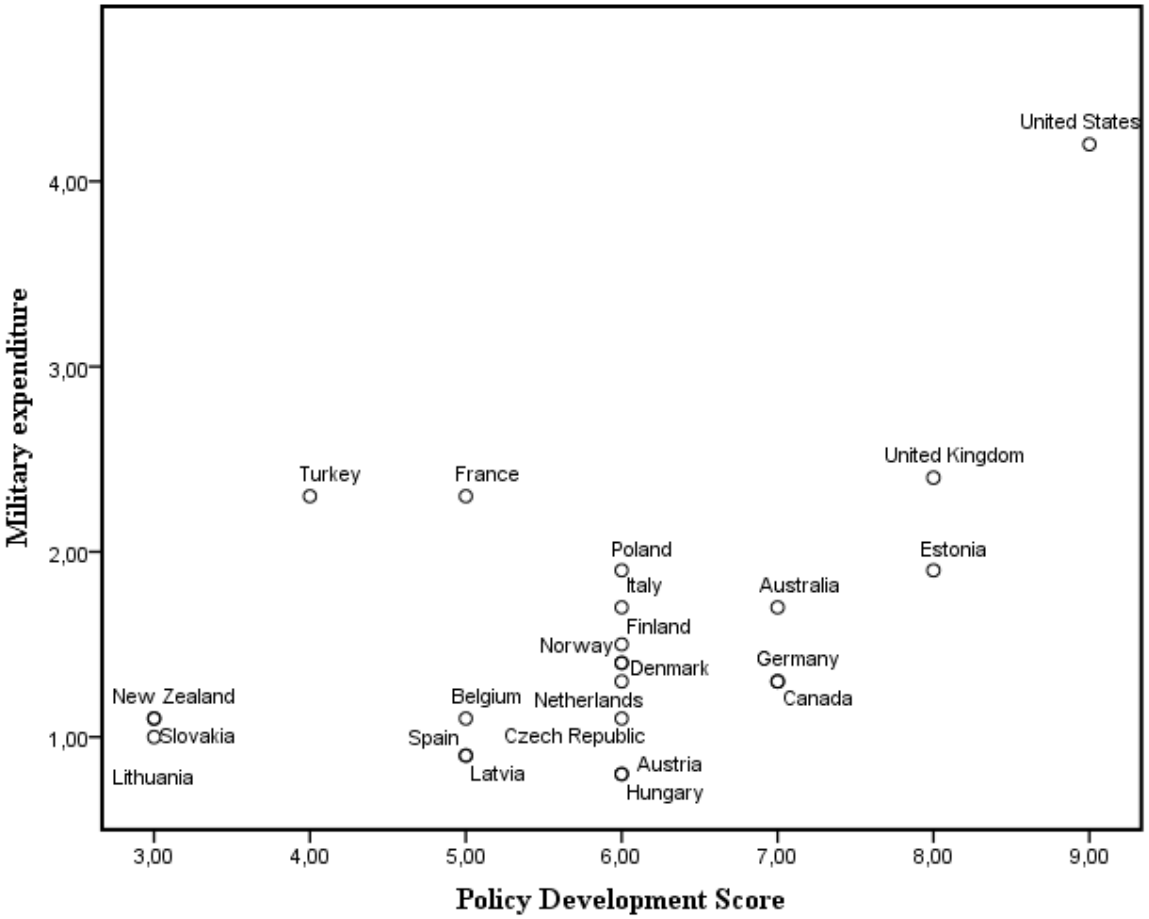
correlation between internet penetration and cyber policy development is apparent.

For future research it might be beneficial to not use internet penetration as the independent variable. The usage of e-government is expected to be more precise. For example, Estonia has a high rate of e-government, which might explain its relatively high score on the country development scale. The reason for this is the fact that internet penetration itself might not affect government policies as much as e-government itself as the latter is actually part of a government's policies, whereas internet usage is expected to rely on multiple factors.

5.4 Military expenditure

Taken as whole, the model as an entity is significant. For military expenditure the *p* value = .005 and hence indicates a statistically significant relation; .005 < .05. Therefore military expenditure appears to be influential for the cybersecurity policy development of a country. Overall a positive correlation is visible as b_2 military expenditure = 1.16. Furthermore, the observed value for *t* is 3.161.

Figure 4: Military Expenditure



The standardized Beta for military expenditure is .559 compared to .313 for internet penetration. This indicates that military expenditure has a higher degree of importance in the model. As a result, military expenditure is found to be the most important indicator within this research. The variable has the highest degree of importance, a positive relation and a it can be concluded that military expenditure makes a significant contribution to the level of a country's cybersecurity policy development.

Figure 4 illustrates that all countries with a policy development score of 7 or higher spend at least 1.3 percent of their GDP on military expenditure. These are countries 4 and 10, Canada and Germany, which spend 1.3 percent of their GDP on military expenditure in 2012. The United States and Great Britain are the primary example of the relation between military expenditure and cybersecurity policy development. Additionally, Lithuania, Slovakia and New Zealand have a relatively low level of military expenditure and a low level of cybersecurity policy development which also corresponds to the expectations.

The country analyses show different approaches to cybersecurity. Some countries, as expected, view cybersecurity in a more conventional manner, in as much as it has become part of their overall military strategy. Other countries show a more novel approach and are developing or have developed their framework accordingly. Nevertheless, although different approaches are visible, this does not directly translate into a lower development of their cybersecurity policy. Rather, the differences indicate a path chosen and do not necessarily influence their level of development.

The United States has by far the biggest percentage of military expenditure in terms of Gross Domestic Product (GDP), with its 4.2 percent no other country comes even close. The other countries with a high percentage of military expenditure are the United Kingdom with 2.4 percent, and France and Turkey 2.3 percent each. The United States and the United Kingdom have an overall score of 9 and 8 respectively, indicating that cybersecurity has almost completely become integrated. However, France has a score of 5 and Turkey of 4; indicating that both countries are still implementing changes.

The countries with the lowest percentage of military expenditure in terms of GDP are Austria and Hungary with 0.8, and Latvia and Spain with 0.9 percent. Nevertheless, these countries do not score significantly lower compared to Austria and Hungary which have an overall score of 6 and Latvia and Spain of 5. Thus, a link between military expenditure and policy development is visible. However, military expenditure is not directly translatable into a higher development in the area and hence more factors influence this development.

5.5 Technological development

Table 7 and 8 contain the multiple regression output. Table 7 and the first table in appendix P includes all three independent variables and provides information on the overall quality of the model. The *R* value represent the 'multiple correlation coefficient' and is called the 'multiple *R*'. The "multiple *R* is the correlation between the observed values of *Y* and the values of *Y* predicted by the multiple regression model" (Field, 2009, pp. 211). In other words, for this research the multiple *R* expresses the correlation between the obtained policy development score and the expected policy development score based upon the predications.

A significant correlation between the level of technological development, internet penetration and military expenditure of a country and its level of cybersecurity policy development is visible, R =.69. The R^2 value indicates "how much variance is explained by the model compared to how much variance there is to explain in the first place" (Field, 2009, pp. 209). The R^2 value = .47 and indicates that 47% of the changes in the level of policy development can be explained with the use of the indicators.

If another independent variable is included, the correlation between that variable and the outcome variable is expected to be larger than 0. Therefore, the adjusted R^2 indicates the level of variance in the policy development score "if the model had been derived from the population from which the sample was taken" (Field, 2009, pp. 221). Overall, 38.6% of the variation in *Y* can be explained by the model; adjusted R^2 = .39.

Table 7: Multiple regression analysis - ANOVA

	Sum of squares	df	Mean Square	F	Sig.
Regression	25.32	3	8.44	5.61	.006
Residual	28.59	19	1.51		
Total	53.91	22			

Note: R= .69, R^2 = .47, Adjusted R^2 = .39

The model appears to improve the prediction as the mean square for the model (MS_M) is large in comparison with the residual mean square (MS_R). The *F*-value is the outcome of MS_M divided by MS_R and hence should be larger than 1, which is the case for the model. Overall, there is a .7 percent "chance that an *F*-ratio this large would happen if the null hypothesis

were true"; $F = 5.61$ which is significant at $p < .007$. Furthermore, an overall significance of .006 ($p = .006$) is visible. Given that $p < .05$ the model as a whole can be regarded as significant.

The coefficients table shows the contribution of the independent variables rather than the overall significance of the model. The coefficient table illustrates that $b_0 = 5.31$, predicting a policy development score of 5.31 if X is 0. Furthermore, the b values for the independent variables can be seen which indicates "the change in the outcome associated with a unit change in the predictor" (Field, 2009, pp. 208).

For technological development the *b value is* -.71 ($b_1 = -.171$). What this indicates is a negative correlation; if the level of technological development of a country increases the level policy development is would decrease. The significance of technological development is .089 ($p = .089$). For an independent variable to be statistically significant the p value must be lower than .05 ($p < .05$). Given the results, the level of technological development is not significantly important.

Table 8: Multiple regression analysis – coefficients

Variable	B^*	$SE\ B^*$	β^{**}	t	p
Constant	5.31	3.16		1.68	.109
Internet Penetration	.003	.03	.025	.11	.915
Military Expenditure	1.003	.36	.48	2.79	.012
Level of Technological Development	-.71	.397	-.42	-1.79	.089

Note: $R^2 = .47$, Adjusted $R^2 = .39$, * Unstandardized coefficient, ** Standardized coefficient

Thus, the regression does not indicate a significant correlation between technological development and cybersecurity policy development. The linear regression is inconclusive and does not appear to provide any statistically relevant data. The regression shows, if any, a negative relation rather than a positive correlation between technological development and cybersecurity policy development. The source of the problem can possibly lie in the sample chosen. All countries chosen are developed and are concerned with threats to their cyberspace and cybersecurity in general – as this was one of the conditions for inclusion in the analysis.

In the analysis no countries with a low level of development were included. Therefore, the 5th category does not appear in the data in appendix G and C, and hence the results may vary for other sample groups. The level of technological difference between the countries is not exceptionally big.

The only country with a below average level of technological development is Turkey. Additionally, Poland, Slovakia, Lithuania, Latvia, and Hungary have an average level of technological development. Out of these countries, Slovakia and Lithuania have a total score of 3, and Turkey has an overall score of 4 out of 9, which indicates a significantly low total. However, the Czech Republic, Poland and Hungary have a score of 6, comparable to countries such as Austria, Finland, and Norway – who all have a high level of technological development.

Furthermore, New Zealand has a total score of 3, even though the country has an above average level of technological development. Therefore, for the sample group no significant relation between technological development and the level of cybersecurity policy development is noticeable. Indicating that technological development is not a primary determinant of a country's cybersecurity policies. Hence, the level of technological development does not appear to be a good indicator and is best left out of the regression.

If technological development is left out and Gross Domestic Product (GDP) per capita is introduced, no correlation is apparent either. Therefore, cyber policy development and both economic and technological development are not interrelated. No significant relation can be drawn from the data. For future research the model might benefit from the inclusion of the 'openness' of a country's economy rather than technological development or economic development itself. Country's with an open economy are expected to be more vulnerable to cyberattacks rather than closed economies and hence the inclusion might yield more fruitful results.

5.6 Limitations of the quantitative analysis

Overall, the model appears to meet most of the assumption. There are however two main problems. First of all, the use of a categorical variable with more than two categories is not in accordance with strict multiple regression rules. Secondly, the sample size of $n = 23$ does not fit the strict rules of regression analysis.

One of the biggest problems with violating assumptions is the fact that the findings are more difficult to generalize (Field, 2009). The important thing to note here is that the

quantitative analyses would benefit from future research which extent the scope. An increase in the number of cases, in essence countries, would allow for more generalization and validation of the findings. Furthermore, additional well-defined and in-depth case studies will help to determine whether or not the outcomes of this research are actually caused by the processes described. Finally, as the field of cybersecurity is constantly evolving, more data is likely to become available or declassified in the future. Most of the data is currently only accessible to a limited group of people given the sensitivity of the information.

As stated above, no data on technological development was readily available and hence more detailed investigation could help to determine the actual effect of this variable. Additionally, other possible determinants, such as the use of e-governance, are worth analyzing in relation to the level of cybersecurity policy development.

At the moment of writing the literature on cybersecurity was relatively limited and not highly coherent. There is much debate and disagreement as discussed in chapter 1 and 2. Therefore, more research on the nature and motivations behind cybersecurity policymaking is encouraged. The current studies are often limited to a single or couple of countries. As countries are aiming to cooperate in this field, additional research might prove to be beneficial. Nevertheless, to use the words of Piketty (2014) “although the information is not perfect, it has the merit of existing” (pp. 16).

6. Case-study: the Netherlands and Denmark

The differences in approach, as discussed in chapter 2.2, did not result into the expected differences in policy development score. Table 8 shows that the independent variables for Denmark and the Netherlands are similar. Both countries have an internet penetration on 93 users per 100 inhabitants. Furthermore, the military expenditure percentages, in terms of GDP, are almost equal. Based on the country analyses, both the Netherlands and Denmark score 6 out 9 possible points. This is a result of the fact that the countries are at level 2 for each of the three dimensions.

Consequently, the two countries are at the implementation level for each of the three dimensions and appear to both be on track with their cybersecurity policy development. However, the different approaches has resulted into a different execution and hence to different situations. This section closely examines the differences and similarities between the two countries. The question underlying this chapter is "how can the different approach lead to similar outcomes?"

Table 9: Case-study matrix

Country	Netherlands	Denmark
Level of technological development	Above average	High
Military expenditure in 2012 (% GDP)	1,3	1,4
Number of internet users in 2012 (per 100 inhabitants)	93	93
Level of cybersecurity development	Implementation	Implementation

The legal framework of Denmark and the Netherlands was ranked at level 2. Although both countries received the same score, this does not mean that they took the same approach. The Netherlands and Denmark appear to differ to some extent in their attitude and perspective towards cybersecurity. Denmark can be regarded as a more military conventional country. Cybersecurity is seen as a new and emerging threat, which has potentially devastating effects on the country. However, the government is aware of the threats and is taking measures to protect the country's critical infrastructure and networked systems. For this end, the national strategy paper lists cybersecurity as one of the new concerns and primary aims (Järvinen, 2014).

Contrary to the Danish approach, the Netherlands has issued two primary National Cyber Security strategy papers. The importance of this has been stressed in chapter 2. With a separate document the focus and plans are more clear and detailed. The issue – in this case protecting cyberspace – is given more weight when discussed separately. Additionally, given that the first 'National Cyber Security Strategy', named strength trough cooperation, was published in June 2011 hints at the relatively early awareness of the topic. As the title indicates, the first strategy paper aimed to improve cooperation amongst allied nations for the protection of cyberspace. The more recent strategy paper, from awareness to capability, was published in October 2013. Within both strategy papers the Dutch government clearly indentifies the most important threats to its cyberspace and digital behavior, something which is less clear in the Danish documents.

Denmark has a different agency responsibility compared to the Netherlands. Denmark has created a Governmental Computer Emergency Response Team service (GovCERT). GovCERT is responsible for the Danish critical infrastructure and government institutions. At the start, GovCERT fell under the responsibility of the Ministry of Science, Technology and Innovation. The authority of GovCERT changed in 2011 and became part of the Danish Defense Intelligence Service. The Danish government continued to reform its agency responsibility and created the 'Centre for Cyber Security'. The new centre absorbed the GovCERT and hence was granted a wider mandate and more responsibility. The Centre no longer is solely responsible for government institutions but is granted more monitoring power. The centre is allowed to monitor public institutions and private companies (Järvinen, 2014).

In the second strategy paper the Dutch government states that it, similar to the Danish government, included their GovCERT into the National Cyber Security Centre. The Dutch Cybercrime Information Hub has not been incorporated into the NCSC, and will continue to function under the Centre for the Protection of National Infrastructure (CPNI) (Ministry of Security and Justice, 2011). In contrast with Denmark, the Dutch government has separated the NCSC from its intelligence and security services. This grants the NCSC a more independent position and reveals the different approach taken by the two countries. The cyber capabilities of the intelligence and security services are 'combined in the Joint Sigint Cyber Unit (JSCU) (Ministry of Security and Justice, 2013).

This different approach has resulted into a situation where the Danish cyber strategy is more capable of defensive and military actions, as this is a primary aim of the government. The Dutch strategy has led to the creation of an expertise centre, which aid both the private and public sector and attempts to bring the sectors together. However, the actual military

capabilities are somewhat behind that of the Danish service. The Dutch government is resolving this issue by transforming the NCSC into a Security Operations Centre as it sees the increasing need of military capabilities.

Overall, the strategy of Denmark is primarily defensive and more military focused when compared to that of the Dutch government. The Danish government developed its cyber strategy based upon defensive capabilities; the focus is on protecting computer systems, especially military computer systems, from illegitimate intrusions, exploitation and interruption. Offensive cyber capabilities are not a primary aim, as a result, response mechanisms and reactionary action is quite limited. Thus, the military is to be protection from attacks without necessarily taking action against these attacks. The literature review indicated the difficulty with both defensive behavior and retaliation.

A hacker or cybercriminal is hard to trace, as the IP addresses are often protected or untraceable. Therefore, the source of an attack is not easily determined. Consequently, focusing on protection rather than action can be a viable option. Nevertheless, the literature also pointed out that unhackable software is an illusion. The attacker generally has the advantage and often it is only a matter of time until a system is breached. The Dutch government has separated its intelligence and security service from its cyber centre and is increasingly paying more attention to military capabilities.

With regards to international cooperation, Denmark is actively pursuing a Nordic collaboration with Norway, Sweden and Finland. As O'Dwyer (2012) states "Nordic governments have identified cyber defense as a fundamental area for urgent cooperation and the development of joint countermeasures, plans and strategies" (pp. 1). This collaboration is planned to take form in the upcoming years. However, for this collaboration to materialize, the individual governments will have to significantly commit to cyber defense and hence develop effective and dedicated 'national military cyber defense centers'. For this end, the Danish government has reached an agreement to provide its cyber defense centre with around 30 to 35 million DKK annually.

Finally, Denmark has become aware of the need for 'offensive military operations in cyberspace', and therefore, will develop plans to increase this capacity in the future (Danish Government, 2012; O'Dwyer, 2012). One of the major differences between the two Dutch cyber strategy papers is the fact that the first was primarily aimed at raising awareness; to make both the public and private sector aware of the lurking threats, and the second is aimed to operationalize the plans of the Dutch government.

Therefore, the Dutch government aims to increase its cooperation with other countries

and significantly values European attempts. The Dutch strategy is primarily focused on information sharing and increasing ICT practices. Furthermore, the second cyber strategy states that “the Netherlands aims to develop a hub for expertise on international law and cybersecurity. The goal of the hub for expertise is to promote the peaceful use of the digital domain (Ministry of Security and Justice, 2013, pp. 10).

The Country Analysis Model helps to classify countries and the level of maturity based upon the three dimensions, but is not supposed to force a specific strategy on a country. The case-study of the Netherlands and Denmark points out a crucial aspect, which is also discussed above; countries should pursue a strategy that best suits their national demands. The field of cybersecurity is relatively novel and hence no ‘grand-strategies’ have been determined. To come back to the question “how can the different approach lead to similar outcomes?”. To conclude, the above analysis has shown that although both countries are currently implementing their cyber policies, the approach taken is often different and tailored to fit the national strategies.

The Danish government appears to have a more conventional approach and military strategy with regards to cybersecurity. Cybersecurity is seen as part of their overall military strategy and valued along with other ‘newly emerging threats’ such as those to the Arctic and from terrorists. Furthermore, the focus of cyber defense, which is separate from cybersecurity in general – as discussed in chapter 2 – might lead to a less coherent framework for Denmark. The Dutch government is primarily focused on knowledge sharing and values the notion of expertise centers. Although the Netherlands is attempting to increase its military capabilities, this does not arise as the primary aim from the two National Cyber Security Strategy documents.

Overall, the different approach of the Danish and Dutch governments did not result into a different level of cybersecurity policy. As both countries are still at the implementation stage for each of the three dimensions, the actual outcome of the approaches taken cannot currently be evaluated. Therefore, the process set into motion in the two countries has uncertain end results and the future will tell which approach is more suitable for contemporary cybersecurity.

7. Conclusion

One of the main problems encountered for the field of cybersecurity is the disagreement about the nature of cyber risks. Authors and policymakers differ in their perspective on the effect of potential attacks. Whereas some argue that cyberspace is the new battleground, others argue that cyberattacks will only serve a secondary function with traditional military capabilities remaining the most important. Whether or not cyberspace will be a new instrument or the primary instrument for governments is uncertain.

What is clear however is that cybersecurity is changing the current status quo. Governments are spending enormous amounts of money of new cyber capabilities and are training an unprecedented number of ICT professionals. Nevertheless, the terminology used and protocols followed are diverse and this has created a plurality of approaches. Consequently, this resulted fragmented policies the existence of many different cybersecurity frameworks.

Educated cyber behavior is becoming increasingly important and many governments have made it a primary aim to raise awareness and train their officials and bureaucrats as well as the general public and companies. Overall, a chain is only a strong as its weakest link'. This somewhat cliché statement is very relevant for cybersecurity. It only takes one mistake, the opening of an infected email or an outdated security system for a system to be intruded. For this end, a strong cybersecurity framework is crucial as more and more government services and personal information is digitalized.

The countries analyzed are all members or partners of the NATO Cooperative Cyber Defense Centre of Excellence, based in Estonia. Furthermore, all countries are considering to sign of have signed the Budapest Convention. This Council of Europe Convention is the most developed international convention for the area of cybercrimes. The country analyses, which are primarily based on the national and cyber strategy papers, have led to a general understanding of the cyber policy development of the 23 different countries under scrutiny in this research.

For the analyses the Country Development Model was used and allowed for a ranking of the countries based upon three dimensions; legal foundation, agency responsibility, and international cooperation. These areas are also highlighted in the Budapest Convention and allowed for a sensible rating of the countries.

The analyses exposed the differences between the countries and their level of development. The bottom three countries are Lithuania, Slovakia and New Zealand. These

countries are at level 1 – policies – for all three dimensions. Although these countries have raised awareness and regard cybersecurity as a security problem their development of cyber policies is fairly limited. The analyses further highlighted a large group, primarily comprised or Western and Northern states which are at level 2 for each dimension; the implementation stage. This group includes the Netherlands, Denmark, Finland, Austria, Norway and the Czech Republic. All have moved away from the development of policies and are currently taking measures to implement these. Estonia, the United Kingdom, and the United States scored highest.

Estonia and the United Kingdom received 8 out 9 points and are at the integration stage for each level except agency responsibility. The United States is the only country which is at the integration level for each dimension and hence has the most developed set of cybersecurity policies out of all countries analyzed. Arguably, the most important information of the analyses is the different approaches taken by the different countries. Whereas some regard military capabilities as a primary aim, and hence often have developed their agency responsibility better, others focus more on education, information sharing and creating a legal foundation. This was most visible between Poland and Hungary where both scored 6 out of 9 points, similar to that of Western and Northern block mentioned above, the distribution amongst the dimensions was rather different. Poland is at the integration level for agency responsibility, yet for legal foundation the country is still at level 1. For Hungary the opposite is visible, with a score of 3 at the legal foundation dimension and only 1 for agency responsibility.

The countries analyzed have a different approach for the protection of their cyberspace. As the literature review pointed out, no uniform approach exists and this has led to the implementation of various new policies. The expectation is that the reliance on the use of networked systems, such as the internet, is only going to increase in the future. In addition, most countries appear to be in favor of international cooperation. This is encouraged because cyberspace transcends borders. As a result, an adequate and rigorous set of cybersecurity policies requires cooperation between countries and different sectors. Therefore, continued research in the field of cybersecurity can prove to be beneficial.

The answer to the research question “which factors determine the level of development of a country’s cybersecurity policies?” is not straightforward. However, the findings of the quantitative analyses illustrate that only military expenditure is a determinant of cybersecurity policies. Both the level of technological development and the internet penetration rate of a country are not found to be determinants. Thus, only military expenditure

is found to be statistically significant (p_{me} = .005) and appears to explain some of the variation in the different policy development scores of the 23 countries. Consequently, the model as a whole does not fit the data.

The lack of correlation between internet penetration and cybersecurity policy development can indicate that either governments are not preoccupied or unaware of the possible negative consequences of high internet penetration rates or that they consider it to be the personal responsibility of their citizens. The literature review suggested that countries with a high internet usage were expected to put the issue higher on the agenda when compared to other nations.

Overall, countries with a high internet penetration were expected to have a more rigorous cybersecurity framework. Additionally, differences in internet penetration rates were found to be linked to differences in costs per capita and governments with a high level of internet penetration are likely to be more affected by the costs rather than countries with lower internet penetration rates. Nevertheless, their does not appear to be a correlation or adequate response from the analyzed governments. To find out the exact reasons for this discrepancy between the literature and quantitative findings more research is necessary.

With regards to the level of technological development the consequences are harder to interpret. Although high technological development was found to be an important factor for cybersecurity policy frameworks, no correlation was found. The problem can be two-fold, either the correlation does not exist, or the data used is not suitable for this type of analysis. Similar to the internet penetration rates, additional research might result into more accurate motives for the incoherence between the literature and the findings.

For military expenditure the correlation indicates that in many countries cyber capabilities are considered to be part of a country's military strategies, albeit to different extents in the sample countries. Furthermore, the found correlation is in accordance with the literature and indicates the general trend in which governments are continuously increasing their cybersecurity frameworks in order to counter possible attacks from unfriendly nations and malicious users of the internet. Furthermore, governments appear to consider the internet as a tool for potential warfare which explains the required increases in military expenditure which are necessary for this.

The research and model are subject to some limitations. The inclusion of more cases would help extent the scope and reliability. This would in turn allow for the inclusion of dummies for the categorical variable used and hence meet the necessary assumption for logistic regressions. Furthermore, other independent variables could be included in future

research to find more statistically significant determinants. In particular the number of cyberattacks, when reliable data becomes available, and the use of e-governance in a country are potentially significant determinants.

To conclude, the only influential factor for a country's cyber policies found is military expenditure. This corresponds with the theoretical framework as most countries regard cybersecurity as a military capability. Whether or not cyber capabilities will change the status-quo and will be at the foreground of future wars and conflicts remains to be seen. However, for most decision- and policymakers cyber capabilities play an important role if the formulation of their policies and have raised significant concerns around the world.

8. Limitations

Cyberspace and cybersecurity is multi-faceted and encompasses many actors and domains. This is a problem not unfamiliar with scholar of cybersecurity, for example, Cavelty, Mauer, & Krishna-Hensel (2007) argue that cybersecurity "is a multi-dimensional and multi-disciplinary public policy issue area, not to mention multi-stakeholder participation in policy initiatives" (pp. 4). Although cyberspace and cybersecurity involves many more stakeholders and the division between government, industry and individuals is sometimes blurred the unit of analysis for this research is a country. The argument behind this is that the focus of this research is on the policies pursued by governments and on what factors these theories are based. Therefore, given that the primary interest is on government behavior in contemporary cybersecurity, this approach is most suitable.

Nevertheless, the focus has to be narrowed further, given the scope of this thesis it is impossible to analyze every country in the world. Furthermore, this would additionally be unfeasible and undesirable, given that not all countries have equal access to cyberspace and the digital domain in general. A digital divide is noticeable, and countries with low levels of technological development will therefore have low levels of technological development. The analysis of these countries will not contribute to the understanding of cybersecurity policies. Additionally, the theories used are mainly Western orientated and hence will consequently not necessarily be relevant for developing countries.

Another limitation is related to the limited research which is currently available for the area of cybersecurity. The independent variables chosen are expected to be the most crucial determinants of a country's cybersecurity policy. However, more influential indicators are possible. For example, the number of cyberattacks a country encounters on a yearly basis. When a country is subject to a high level of cyberattacks, which means that its cyberspace is frequently attacked, it might be more likely to increase its cybersecurity. One of the most discussed cases is Estonia. As discussed in the introduction, Estonia was the only Eastern European country rated 4 out 5 stars in the SDA and McAfee report.

Furthermore, Estonia encountered one of the largest recorded cyberattacks in history in 2007, when its main institutions, including parliament and banks, were subject to disruptions (The Economist, 2008). Therefore, the number of attacks is expected influence government's decisions on cybersecurity policy. Nevertheless, reliable data on the number of attacks is not available. First of all, countries are reluctant to publish these numbers as this might expose critical areas of their infrastructure. Furthermore, countries are also unaware of

all the attacks given that most of them are either hidden or not detected by people, or not reported to the authorities.

Finally, internet penetration and technological development did not significantly influence the level of policy development within the sample group. Two possible reasons have been highlighted for this. First of all, future research might benefit from focusing on the usage of e-government activities rather than internet penetration. The former is an actual policy of governments and affects its day-to-day functioning. Whereas the latter is more an individual practice in our contemporary world. Secondly, the units of analysis were all relatively high developed nations. Therefore, the significance might change when other countries are included. The scope of this thesis did not leave space for further investigation and hence future research is highly stimulated.

Bibliography

Arquilla, J., & Borer, D. A. (2007). *Information Strategy and Warfare – A guide to Theory and Practice*. London: Routledge

Australian Government. (2009). *Cyber Security Strategy.* Retrieved may 10, 2014, from http://www.ccdcoe.org/328.html

Australian Government Department of Defence. (2013). *2013 Defence White Paper*. Retrieved may 10, 2014 from http://www.ccdcoe.org/328.html

Bayuk, J. L. (2010). *Enterprise Security for the Executive: Setting the Tone at the Top.* Santa Barbara, CA: Praeger.

Bayuk, J. L., Healey, J., Rohmeyer, P., Sachs, M. H., Schmidt, J., & Weiss, J. (2012). *Cyber Security Policy Guidebook.* New Jersey: John Wiley & Sons, Inc.

Belgian Cyber Security Strategy paper (2012). *Cyber Security Strategy*. Retrieved may 10, 2014 from http://www.ccdcoe.org/328.html

Bowerman, B. L., & O'Connell, R. T. (1990). *Linear Statistical Models: An Applied Approach* (2nd ed.). Belmont, CA: Duxbury.

Braithwaite, T (2001) Executives need to know: the arguments to include in a benefits justification for increased cyber security spending. *Information Systems Security*, *10*(4), 1-14.

Button, M. (2009). *Doing Security: A Critical Reflection and an Agenda for Change.* Palgrave Macmillan.

Buzan, B., Waever, O., & de Wilde, J. (1998). *Security: A New Framework for Analysis.* Lynne Rienner Publishers.

Cabinet Office United Kingdom. (2011). *The UK Cyber Security Strategy. Protecting and Promoting the UK in a Digital World*. Retrieved May 22, 2014 from http://www.ccdcoe.org/328.html

Cavelty, M. D., Mauer, V., & Krishna-Hensel, S. F. (2007). *Power and Security in the Information Age - Investigating the Role of the State in Cyberspace.* Hampshire, England: Ashgate Publishing ltd.

Clarke, R. A., & Knake, R. K. (2011). *Cyber War: the Next Threat to National Security and What to Do About It.* HarperCollins Publishers.

Commonwealth of Australia (2013). *2013 National Security Strategy*. Retrieved may 10, 2014 from http://www.ccdcoe.org/328.html

Cortina, J. M. (1993). What is coefficient alpha? An examination of theory and application.

Journal of Applied Psychology, 78(1), 98-104.

Council of Europe. (2014). *Convention on Cybercrime*. CETS No.: 185. Retrieved February 10, 2013, from http://conventions.coe.int/

CybercrimeData AS. (2014). Cybercrime laws. Retrieved May 20, 2014 from http://www.cybercrimelaw.net/Cybercrimelaws.html

Czech Republic. (2011). *Strategy of the Czech Republic in the Field of Cybernetic Security for 2012-2015.* Retrieved may 12, 2014 from http://www.ccdcoe.org/328.html

Czech Republic. (2013). *Draft Act of Cyber Security.* Retrieved may 12, 2014 from http://www.ccdcoe.org/328.html

Danish Government. (2012). *Danish Defence Agreement 2013-2017.* Retrieved may 12, 2014 from http://www.ccdcoe.org/328.html

DCAF. (2005). Backgrounder security governance and reform – national security policy. *Geneva: Backgrounder Series.*

Dutch Ministry of Security and Justice. (2011). *The National Cyber Security Strategy: Strength through cooperation*.

Dutch Ministry of Security and Justice. (2013). *The National Cyber Security Strategy: from awareness to capability.*

Farrell, H. (2014). The political science of cyber security III – how international relations theory shapes U.S. cyber security doctrine. The Washington Post.

Federal Chancellery Digital Austria. (2012). *National ICT Security Strategy*. Retrieved may 10, 2014 from http://www.ccdcoe.org/328.html

Federal Ministry of Interior Germany. (2011). *Cyber Security Strategy for Germany*. Retrieved may 15, 2014 from http://www.ccdcoe.org/328.html

Field, A. (2009). *Discovering Statistics Using SPSS*. SAGE Publications Ltd.

FireEye. (2013). The advanced cyber attack landscape. *FireEye Inc*. Retrieved February 10, 2014, from http://www2.fireeye.com/WEB2013ATLReport.html.

Florida, R., Mellander, C., Stolarick, K., Silk, K., Matheson, Z., & Hopgood, M. (2011). Creativity and prosperity: the global creativity index. *Martin Prosperity Institute.*

French Network and Information Security Agency. (2011). *Information Systems Defence and Security - France's Strategy*. Retrieved may 15, 2014 from http://www.ccdcoe.org/328.html

Fritz, J. (2008). How China will use cyber warfare to leapfrog in military competitiveness. *Culture Mandala: The Bulletin of the Centre for East-West Cultural and Economic Studies*, *8*(2), 22-80.

Fischer, E. A. (2009). *Creating a National Framework for Cyber security: An analysis of Issues and Options.* New York: Nova Science Publishers Inc.

Gartzke, E. (2013). The myth of cyberwar: brining war in cyberspace back down to earth. *International Security, 38*(2), 41-73.

Government of Canada. (2010). *Canada's Cyber Security Strategy: for a Stronger and More Prosperous Canada*. Retrieved may 10, 2014 from http://www.ccdcoe.org/328.html

Government of Canada. (2013). *Action plan 2010-2015 for Canada's Cyber Security Strategy.* Retrieved may 10, 2014 from http://www.ccdcoe.org/328.html

Government of Finland. (2013). *Finland's Cyber Security Strategy*. Retrieved may 16, 2014 from http://www.ccdcoe.org/328.html

Government of France. (2013). *White Paper: Defence and National Security*. Retrieved may 15, 2014 from http://www.ccdcoe.org/328.html

Government of Hungary. (2012). *Hungary's National Security Strategy*. Retrieved may 15, 2014 from http://www.ccdcoe.org/328.html

Government of Hungary. (2013). *National Cyber Security Strategy of Hungary*. Retrieved may 15, 2014 from http://www.ccdcoe.org/328.html

Government of Latvia. (2010). *Law on the Security of Information Technologies.* Retrieved may 17, 2014 from http://www.ccdcoe.org/328.html

Government of the Republic of Lithuania. (2011). *Programme for the Development of Electronic Information Security for 2011–2019.* Retrieved may 17, 2014 from http://www.ccdcoe.org/328.html

Government of the Republic of Poland. (2013). *Cyberspace Protection Policy of the Republic of Poland*. Retrieved may 19, 2014 from http://www.ccdcoe.org/328.html

Government of the Slovak Republic. (2008). *National Strategy for Information Security in the Slovak Republic*. Retrieved may 19, 2014 from http://www.ccdcoe.org/328.html

Grauman, B. (2012). Cyber-security: the vexed question of global rules. Brussels: *Security and Defense Agenda*.

Hathaway, M. E., & Klimburg, A. (2012). Preliminary Considerations: On National Cyber Security. In Klimburg, A. (Eds.), *National cyber security: framework manual*, 1-43.

Her Majesties Government United Kingdom. (2010). *A Strong Britain in an Age of Uncertainty: The National Security Strategy*. Retrieved May 22, 2014 from http://www.ccdcoe.org/328.html

Järvinen, H. (2014). Danish government plans to create a Centre for Cybersecurity with privacy-invasive powers. *EDRi.* Retrieved June 10, 2014, from http://edri.org/danish-

government-plans-create-center-cybersecurity-privacy-invasive-powers/

Jervis, R. (1987). Cooperation under the security dilemma. *World Politics, 30*(2), 167-214.

Joint media release. (September 15, 2011). Retrieved may 10, 2014 from http://foreignminister.gov.au/releases/Pages/2011/kr_mr_110916.aspx?ministerid=2

Katsikas, S. K. (2005). Assuring critical information infrastructure. *Cyberspace Security and Defense: Research Issue,* 43-55

Kello, L. (2012). *Cyber disorders: rivalry and conflict in a global information age*. Belfer Center: Harvard Kennedy School

Kello, L. (2013). The meaning of the cyber revolution: perils to theory and statecraft. *International Security, 38*(2), 7-40.

Kellstedt, P. M., & Whitten, G. D. (2007) *The Fundamentals of Political Science Research,* Cambridge: Cambridge University Press.

Kim, H. S., Wang, Q. H., & Ullrich, J. B. (2012). A comparative study of cyberattacks. *Communications of the ACM, 55*(3), 66-73.

Kingdom of Denmark. (2013). Danish Defense Agreement 2013-2017. Retrieved April 18, 2014 from http://www.ccdcoe.org/328.html.

Lehnert, M., Miller, B. & Wonka, A. (2007). Increasing the relevance of research questions: considerations on theoretical and social relevance in political science. In Gschwend, T. & Schimmelfennig, F. (Eds.), *Research Design in Political Science: How to Practice What They Preach.* Pp. 21-33.

Lewis, J.A. (2002). Assessing the risks of cyber terrorism, cyber war and other cyber threats. *Centre for Strategic and International Studies.*

Libicki, M. C. (2007). *Conquest in Cyberspace: National Security and Information Warfare.* Cambridge University Press.

Lynn, W. J. (2010). Defending a new domain – the pentagon's cyberstrategy. *Foreign Affairs*

Menting, M. A. (2011). Cybercrime Laws By Country & Other Resources.

Ministry of Defence Estonia. (2008). *Cyber Security Strategy.* Retrieved may 15, 2014 from http://www.ccdcoe.org/328.html

Ministry of Defence The Netherlands. (2012). *The Defence Cyber Strategy*. Retrieved May 17, 2014 from http://www.ccdcoe.org/328.html

Ministry of Transport, Maritime Affairs and Communications Turkey. (2013). National Cyber Security Strategy and 2013-2014 Action Plan. Retrieved may 21, 2014 from http://www.ccdcoe.org/328.html**.**

Mueller, M., Schmidt, A., & Kuerbis, B. (2013). Internet security and networked governance

in international relations. *International Studies Review 15*(1), 86-104.

National Coordinator for Security and Counterterrorism The Netherlands. (2013). *National Cyber Security Strategy 2: From Awareness to Capability.* Retrieved April 19, 2014 from http://www.ccdcoe.org/328.html

NATO. (2012). *Defending against cyber attacks*. Retrieved January 29, 2014, from http://www.nato.int/cps/en/natolive/75747.htm

NATO. (2013). *Defense Ministers Press Conference*. Retrieved June 10, 2014, from http://www.nato.int/cps/en/natolive/opinions_101151.htm

NATO. (2014). NATO Review Magazine. Retrieved May 12, 2014 from http://www.nato.int/docu/review/2014/EDITORIALTEAM/EN/index.htm

New Zealand Government. (2011). *New Zealand's Cyber Security Strategy*. Retrieved May 17, 2014 from http://www.ccdcoe.org/328.html

Norwegian Ministries. (2012). *Cyber Security Strategy for Norway*. Retrieved May 17, 2014 from http://www.ccdcoe.org/328.html

Nye, J. S. (2012). Cyber war and peace. *Project Syndicate*. Retrieved February 5, 2014, from http://www.project-syndicate.org/commentary/cyber-war-and-peace#m3hc0IPIFKhGpCFU.99

O'Dwyer. (2012). Cyber defense takes center stage in Nordic Cooperation. *DefenseNews.* Retrieved June 10, 2014 from http://www.defensenews.com

OECD. (2005). OECD input to the United Nations working group on internet governance. Retrieved from http://www.oecd.org/internet/ieconomy/e-bookoecdinputtotheunitednationsworkinggrouponinternetgovernance.htm#for

Peduzzi, P., Concato, J., Kemper, E., Holford, T.R., & Feinstein, A.R. (1996). A simulation study of the number of events per variable in logistic regression analysis. *Journal of Clinical Epidemiology, 49*(12), 1373-1379.

Piketty, T. (2014). *Capital in the Twenty-First Century*. Cambridge, UK: The Belknap Press of Harvard University Press.

Presidency of the Council of Ministers Italy. (2013). *National Strategic Framework for the Security of Cyberspace.* Retrieved may 15, 2014 from http://www.ccdcoe.org/328.html

Ralston, P.A.S., Graham, J.H., & Hieb, J.L. (2007). Cyber security risk assessment for SCADA and DCS networks. *ISA Transactions, 46*(1), 583-594.

Rueter, N. C. (2011). *The cybersecurity dilemma*. Duke University: department of political science.

Scruggs, L.A. (1999). Institutions and environmental performance in seventeen Western democracies. *British Journal of Political Science, 29*(1), 1-31.

Sharma, A. (2010). Cyber wars: a paradigm shift from means to ends, *Strategic Analysis 34*(1), 62-73.

Spanish Cyber Security Institute. (2013) *National Cyber Security: a Commitment for Everybody*. Retrieved May 19, 2014 from http://www.ccdcoe.org/328.html

Stevens, J. (2002). *Applied Multivariate Statistics for the Social Sciences* (4th ed.). Hillsdale, NJ: Erlbaum.

The Economist. (2008). Marching off to cyberwar. *Technology Quarterly, 4*.

UK Cabinet Office (2009). *Cyber security strategy of the United Kingdom: safety, security, and resilience in cyber space*. UK, London: The Stationary Office.

United States of America. (2009). *Cyberspace Policy Review*. Retrieved may 22, 2014 from http://www.ccdcoe.org/328.html

United States of America. (2011). *International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World.* Retrieved may 22, 2014 from http://www.ccdcoe.org/328.html

United States of America. (2011). *Department of Defense Strategy for Operating in Cyberspace.* Retrieved May 22, 2014 from http://www.ccdcoe.org/328.html

UNODC. (2013). *Comprehensive Study On Cybercrime*. New York, USA: United Nations.

VanVoorhis, C.W. & Morgan, B.L. (2001). Statistical rules of thumbs: what we don't want to forget about sample sizes. *Psi Chi Journal of Undergraduate Research, 6*(4), 139-141.

VanVoorhis, C.W. & Morgan, B.L. (2007). Understanding power and rules of thumb for determining sample sizes. *Tutorials in Quantitative Methods for Psychology, 3*(2), 43-50.

Vittinghoff, E., & McCulloch, C.E. (2006). Relaxing the rule of ten events per variable in logistic and Cox regression. *American Journal of Epidemiology, 165*(6), 710-718.

Walt, S. M. (2010). Is the cyber threat overblown? *Foreign Policy.* Retrieved February 8, 2014, from http://www.foreignpolicy.com/posts/2010/03/30/is_the_cyber_threat_overblown

Walter, B.F. (1997). The critical barrier to civil war settlement. *International Organization, 51*(3), 335-364.

Weimann, G. (2004). Cyberterrorism: how real is the threat? Washington DC, USA: *United States Institute of Peace.*

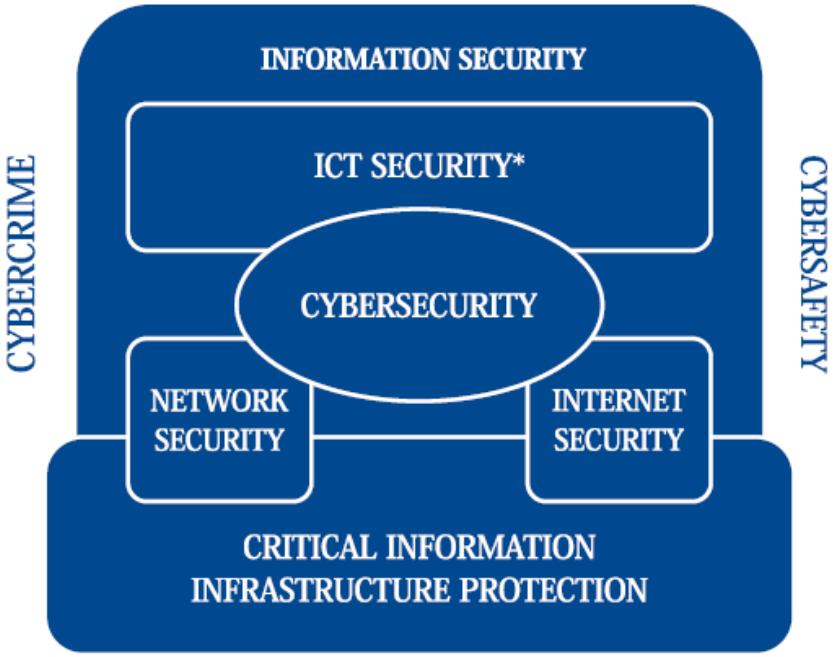
Xiao-yan, G., Yu-qing, Y., & Li-lei, L. (2011). An information security maturity evaluation

mode. *Procedia Engineering, 24,* 335-339.

Xu, K., Duan, Z.L., Zhang, Z., & Chandrashekar, J. (2004). On properties of internet exchange points and their impact on AS topology and relationship. In *NETWORKING 2004. Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless Communications* (pp. 284-295). Springer Berlin Heildeberg.

Zwolski, K., & Kaunert, C. (2011). The EU and climate security: a case of successful norm entrepreneurship? *European Security, 20*(1), 21-43.

Appendix A



Source: Hathaway & Klimburg, 2012

Appendix B: National (Cyber) Security Strategies in Selected OECD Countries

Table 3: National (Cyber) Security Strategies in Selected OECD Countries

	NATIONAL SECURITY			CYBER SECURITY			NATIONAL CYBER SECURITY
	Document	Year	Basic Definition / Understanding	Document	Year	Basic Definition / Understanding	Key Objectives / Areas
AU	The First National Security Statement to the Parliament[88]	2008	'Freedom from attack or the threat of attack; the maintenance of our territorial integrity; the maintenance of our political sovereignty; the preservation of our hard won freedoms; and the maintenance of our fundamental capacity to advance economic prosperity for all Australians.'	Cyber Security Strategy[89]	2009	'Measures relating to the confidentiality, availability and integrity of information that is processed, stored and communicated by electronic or similar means.'	Three key objectives: - 'All Australians are aware of cyber risks, secure their computers and take steps to protect their identities, privacy and finances online' - 'Australian Businesses operate secure and resilient informations and communications technologies to protect the integrity of their own operations and the identity and privacy of their customers' - 'The Australian Government ensures its information and communications technologies are secure and resilient'
CA	Securing an Open Society: Canada's National Security Policy[90]	2004	'National security deals with threats that have the potential to undermine the security of the state or society. These threats generally require a national response, as they are beyond the capacity of individuals, communities or provinces to address alone. National security is closely linked to both personal and international security. While most criminal offences, for example, may threaten personal security, they do not generally have the same capacity to undermine the security of the state or society as do activities such as terrorism or some forms of organized crime. Given the international nature of many of the threats affecting Canadians, national security also intersects with international security. At the same time, there are a growing number of international security threats that impact directly on Canadian security and are addressed in this strategy.'	Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada[91]	2010	'detect, identify and recover' from cyber attacks which 'include the unintentional or unauthorized access, use, manipulation, interruption or destruction (via electronic means) of electronic information and/or the electronic and physical infrastructure used to process, communicate and/or store that information. The severity of the cyber attack determines the appropriate level of response and/or mitigation measures: i.e., cyber security.'	Three pillars: - 'Securing Government systems' - 'Partnering to secure vital cyber systems outside the federal Government' - 'Helping the Canadians to be secure online'

DE	White Paper 2006 on German Security Policy and the Future of the Bundes-wehr[92]	2006	'German security policy is based on a comprehensive concept of security; it is forward-looking and multilateral. Security cannot be guaranteed by the efforts of any one nation or by armed forces alone. Instead, it requires an all-encompassing approach that can only be developed in networked security structures.'	Cyber Security Strategy for Germany[93]	2011	'Cyber security and civilian and military cyber security: (Global) cyber security is the desired objective of the IT security situation, in which the risks of global cyberspace have been reduced to an acceptable minimum. Hence, cyber security in Germany is the desired objective of the IT security situation, in which the risks of the German cyberspace have been reduced to an acceptable minimum. Cyber security (in Germany) is the sum of suitable and appropriate measures. Civilian cyber security focuses on all IT systems for civilian use in German cyberspace. Military cyber security focuses on all IT systems for military use in German cyberspace.'	Ten strategic areas (objectives and measures): - 'Protection of critical information infrastructures' - 'Secure IT systems in Germany' - 'Strengthening IT security in the public administration' - 'National Cyber Response Centre' - 'National Cyber Security Council'	- 'Effective crime control also in cyberspace' - 'Effective coordinated action to ensure cyber security in Europe and worldwide' - 'Use of reliable and trustworthy information technology' - 'Personnel development in federal authorities' - 'Tools to respond to cyber attacks'
FR	The French White Paper on Defence and National Security[94]	2008	'The aim of France's National Security strategy is to ward off risks or threats liable to harm the life of the nation. Its first aim is to defend the population and French territory, this being the first duty and responsibility of the State. The second aim is to enable France to contribute to European and international security: this corresponds both to its own security needs, which also extend beyond its frontiers, and to the responsibilities shouldered by France within the framework of the United Nations and the alliances and treaties which it has signed. The third aim is to defend the values of the 'republican compact' that binds all French people to the State, namely the principles of democracy, and in particular individual and collective freedoms, respect for human dignity, solidarity and justice.'	Information systems defence and security: France's strategy[95]	2011	'The desired state of an information system in which it can resist events from cyberspace likely to compromise the availability, integrity or confidentiality of the data stored, processed or transmitted and of the related services that these systems offer or make accessible. Cybersecurity makes use of information systems security techniques and is based on fighting cybercrime and establishing cyberdefence.'	Four strategic objectives: '- Become a cyberdefence world power in cyberdefence - Safeguard France's ability to make decisions through the protection of information related to its sovereignty - Strengthen the cybersecurity of critical national infrastructures - Ensure security in cyberspace'	
NL	Strategie Nationale Veiligheid[96]	2007	[*Own Translation*] 'National security is at stake when the vital interests of our state and/or our society [1. territorial security, 2. economic security, 3. ecological security, 4. physical security, and 5. social and political security] are threatened in such way that it leads to – potential – social disruption. National security contains both the corrosion of security by intentional human action (security) as well as the damage caused by disasters, system or process failures, human error or natural anomalies such as extreme weather (safety).'	The National Cyber Security Strategy (NCSS): Strength through coopera-tion[97]	2011	'Cyber security is freedom from danger or damage due to the disruption, breakdown, or misuse of ICT. The danger or damage resulting from disruption, breakdown, or misuse may consist of limitations to the availability or reliability of ICT, breaches of the confidentiality of information stored on ICT media, or damage to the integrity of that information.'	'Security and trust in an open and free digital society:' The Strategy's goal is to strengthen the security of digital society in order to give individuals, businesses, and public bodies more confidence in the use of ICT. To this end, the responsible public bodies will work more effectively with other parties to ensure the safety and reliability of an open and free digital society. This will stimulate the economy and increase prosperity and well-being. It will ensure legal protection in the digital domain, prevent social disruption, and lead to appropriate action if things go wrong.'	

UK	A Strong Britain in an Age of Uncertainty: The National Security Strategy[98]	2010	'The security of our nation is the first duty of government. It is the foundation of our freedom and our prosperity.' [...] 'The National Security Strategy of the United Kingdom is: to use all our national capabilities to build Britain's prosperity, extend our nation's influence in the world and strengthen our security.'	The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world[99]	2011	actions taken 'to reduce the risk and secure the benefits of a trusted digital environment for businesses and individuals.'	Four objectives: '- The UK to tackle cybercrime and be one of the most secure places in the world to do business in cyberspace - The UK to be more resilient to cyber attacks and better able to protect our interests in cyberspace - The UK to have helped shape an open, stable and vibrant cyberspace which the UK public can use safely and that supports open societie - The UK to have the cross-cutting knowledge, skills and capability it needs to underpin all our cyber security objectives'	
US	National Security Strategy[100]	2010	'Our national security depends upon America's ability to leverage our unique national attributes, just as global security depends upon strong and responsible American leadership. That includes our military might, economic competitiveness, moral leadership, global engagement, and efforts to shape an international system that serves the mutual interests of nations and peoples. For the world has changed at an extraordinary pace, and the United States must adapt to advance ou interests and sustain our leadership.'	The National Strategy to Secure Cyberspace[101]	2003	'protect against the debilitating disruption of the operation of information systems for critical infrastructures and, thereby, help to protect the people, economy, and national security of the United States. We must act to reduce our vulnerabilities to these threats before they can be exploited to damage the cyber systems supporting our Nation's critical infrastructures and ensure that such disruptions of cyberspace are infrequent, of minimal duration, manageable, and cause the least damage possible. Securing cyberspace is an extraordinarily difficult strategic challenge that requires a coordinated and focused effort from our entire society -- the federal government, state and local governments, the private sector, and the American people.'	Three Strategic Objectives: '- Prevent cyber attacks against America's critical infrastructures - Reduce national vulnerability to cyber attacks; and - Minimize damage and recovery time from cyber attacks that do occur.'	
				National Security Presidential Directive 4[102] (partially unclassified)[103]	2008	[*From the 2009 Cyberspace Policy Review*] 'cybersecurity policy [...] includes strategy, policy, and standards regarding the security of and operations in cyberspace, and encompasses the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure. The scope does not include other information and communications policy unrelated to national security or securing the infrastructure.'	[*From the 2008 National Security Presidential Directive 54*] Thirteen Objectives: '- establishing the National Cyber Security Center within the Department of Homeland Security' '- Move towards managing a single federal enterprise network; - Deploy intrinsic detection systems; - Develop and deploy intrusion prevention tools; - Review and potentially redirect research and funding; - Connect current government cyber operations centers;	- Develop a government-wide cyber intelligence plan; - Increase the security of classified networks; - Expand cyber education; - Define enduring leap-ahead technologies; - Define enduring deterrent technologies and programs; - Develop multi-pronged approaches to supply chain risk mariagement; and - Define the role of cyber security in private sector domains.'
				Cyberspace Policy Review. Assuring a Trusted and Resilient Information and Communications Infrastructure	2009			

Source: Hathaway & Klimburg, 2012, pp. 23-25)

Appendix C – Indicator table

Variable / Country	Policies and level of maturity	Level of technological development	Internet penetration (per 100)	Military expenditure (% GDP)
1. Australia	7	High	82,3	1,7
2. Austria	6	High	81,0	0,8
3. Belgium	5	Above Average	82,0	1,1
4. Canada	7	High	86,8	1,3
5. Czech Republic	6	Above Average	75,0	1,1
6. Denmark	6	High	93,0	1,4
7. Estonia	8	Above Average	79,0	1,9
8. Finland	6	High	91,0	1,5
9. France	5	High	83,0	2,3
10. Germany	7	High	84,0	1,3
11. Hungary	6	Average	72,0	0,8
12. Italy	6	Above Average	58,0	1,7
13. Latvia	5	Average	74,0	0,9
14. Lithuania	3	Average	68,0	1,0

15. The Netherlands	**6**	**Above Average**	**93,0**	**1,3**
16. New Zealand	3	Above Average	89,5	1,1
17. Norway	6	High	95,0	1,4
18. Poland	6	Average	65,0	1,9
19. Slovakia	3	Average	80,0	1,1
20. Spain	5	High	72,0	0,9
21. Turkey	4	Below Average	45,1	2,3
22. United Kingdom	8	Above Average	87,0	2,4
23. United States	9	High	81,0	4,2

Source: Florida et. al., 2011; World Development Indicators – World Bank, 2014
Missing NATO members: Albania, Bulgaria, Croatia, Greece, Iceland, Portugal, Slovenia (no information and not included in the NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE); indicating that their policies and documents are not up-to-standard.

Additional countries: Australia, Austria, Finland, New Zealand (included in the CCDCOE)

https://www.ccdcoe.org/328.html

Appendix D- Case-study matrix

Country	Netherlands	Denmark
Level of technological development	Above average	High
Military expenditure in 2012 (% GDP)	1,3	1,4
Number of internet users in 2012 (Per 100)	93	93
Level of cybersecurity development	Implementation	Implementation

Source: World Bank, 2013

Appendix E - Technological development index

COUNTRY	R&D INVESTMENT	RESEARCHERS	INNOVATION	TECHNOLOGY INDEX
Finland	3	1	4	1
Japan	4	3	2	2
United States	6	7	1	3
Israel	1	—	5	4
Sweden	2	2	6	5
Switzerland	5	11	3	6
Denmark	9	5	9	7
Republic of Korea	7	16	—	8
Germany	8	13	7	9
Singapore	11	4	11	10
Canada	13	9	8	11
Norway	18	6	18	12
Austria	12	14	13	13
France	10	15	16	14
Australia	17	8	17	15
Belgium	14	17	15	16
Netherlands	16	18	12	17
United Kingdom	15	—	14	18
New Zealand	25	10	20	19
Ireland	23	19	19	20
Russian Federation	22	12	36	21
Hong Kong	41	26	10	22
Slovenia	20	22	22	23
Spain	29	21	23	24
Czech Republic	21	27	26	25
Italy	27	34	21	26
Estonia	33	20	30	27
Serbia	19	—	59	28
Croatia	24	28	31	29
China	26	39	—	30
Lithuania	36	23	34	31
Portugal	35	24	35	32
Hungary	32	30	24	33
Ukraine	28	—	50	34
Uganda	30	—	72	35
Slovakia	44	25	39	36
Poland	45	29	44	37
Greece	39	32	33	38
Latvia	47	31	42	39
Bulgaria	46	33	41	40

COUNTRY	R&D INVESTMENT	RESEARCHERS	INNOVATION	TECHNOLOGY INDEX
Brazil	31	43	46	41
India	38	36	27	42
Costa Rica	51	—	28	43
Azerbaijan	55	—	65	44
South Africa	34	46	32	45
Armenia	61	—	51	46
Georgia	62	—	45	47
Chile	40	41	55	48
Romania	50	35	52	49
Kyrgyzstan	65	—	66	50
Turkey	37	44	54	51
Philippines	68	—	56	52
Trinidad and Tobago	69	—	40	53
Malaysia	42	45	25	54
Argentina	48	37	37	55
Peru	70	—	61	56
Jamaica	73	—	49	57
Honduras	76	—	64	58
Cyprus	53	40	29	59
Kazakhstan	60	38	63	60
Macedonia	56	42	62	61
Mexico	49	49	—	62
Uruguay	59	47	48	63
Thailand	58	48	47	64
Panama	52	54	53	65
Bolivia	57	53	67	66
El Salvador	—	57	60	67
Viet Nam	64	52	70	68
Sri Lanka	67	51	58	69
Madagascar	63	59	71	70
Paraguay	71	55	69	71
Ecuador	72	58	57	72
Pakistan	66	56	—	73
Indonesia	74	50	—	74
Cambodia	75	60	—	75

Source: Florida, Mellander, Stolarick, Silk, Matheson, & Hopgood (2011)

Appendix F – Score summary

Dimension / Scores / Country	Legal foundation	Agency responsibility	International cooperation	Total score
1. Australia	3/3	2/3	2/3	**7/9**
2. Austria	2/3	2/3	2/3	**6/9**
3. Belgium	2/3	1/3	2/3	**5/9**
4. Canada	2/3	2/3	3/3	**7/9**
5. Czech Republic	2/3	2/3	2/3	**6/9**
6. Denmark	2/3	2/3	2/3	**6/9**
7. Estonia	3/3	2/3	3/3	**8/9**
8. Finland	2/3	2/3	2/3	**6/9**
9. France	1/3	2/3	2/3	**5/9**
10. Germany	2/3	3/3	2/3	**7/9**
11. Hungary	3/3	1/3	2/3	**6/9**
12. Italy	2/3	1/3	2/3	**6/9**
13. Latvia	2/3	2/3	1/3	**5/9**
14. Lithuania	1/3	1/3	1/3	**3/9**
15. The Netherlands	2/3	2/3	2/3	**6/9**
16. New Zealand	1/3	1/3	1/3	**3/9**

17. Norway	2/3	2/3	2/3	**6/9**
18. Poland	1/3	3/3	2/3	**6/9**
19. Slovakia	1/3	1/3	1/3	**3/9**
20. Spain	2/3	1/3	2/3	**5/9**
21. Turkey	1/3	2/3	1/3	**4/9**
22. United Kingdom	3/3	2/3	3/3	**8/9**
23. United States	3/3	3/3	3/3	**9/9**

Appendix G – Detailed country analyses

1. Australia

The Australian government has expressed a significant effort and commitment to the improvement of its cybersecurity policies. The most recent documents – the 2013 National Security Strategy and the 2013 Defense White Paper – repeatedly discuss cyber capabilities and threats. Cybersecurity is both discussed separately and in conjunction with other types of defense and security. The Defense White Paper used the word "cyber" throughout the entire text. The National Cyber Security Strategy, which was published in 2009, was considerable more limited in scope. Significant improvement has been made in the most recent edition. What this indicates is a more serious and committed attitude of the Australian governments towards the protection of its cyberspace.

Legal foundation

Australia has not developed a strong legal foundation with regards to cybersecurity. As the White Paper states: "Australia believes that the existing framework of international law, including the UN Charter and international humanitarian law, applies to cyberspace. Australia is participating in international efforts to achieve a common understanding of these laws" (Australian Government Department of Defence, 2013, p. 21). Furthermore, although cybersecurity is relatively extensively discussed, the perspective of Australia is rather traditional or conventional in as much as it seeks to operate within existing norms, rules, and laws. Nevertheless, Australia has shown a continuous development in the area and has implemented multiple legal reforms and new legislation. Therefore, Australia is currently at level 3.

Agency responsibility

The Australian government established the 'Cyber Security Operations Centre (CSOC) within the Defense Signals Directorate (DSD)'. Nevertheless, the CSOC only addresses one part of the cybersecurity regime. The Australian government has realized this and has "announced the establishment of a new Australian Cyber Security Centre to improve partnerships between government Agencies and with industry. The Centre will bring together cybersecurity capabilities from across the national security community, fully located in one facility" (Australian Government Department of Defence, 2013, p. 21-22). The Australian Cyber Security Centre would include all aspects and branches involved in cybersecurity and entail a

significant improvement. A board will head the Centre which is chaired by the Secretary of the Attorney-General's Department. Thus, although efforts are made much still needs to be done. Currently, the organizations is scattered and a clear and detailed action plan is absent. Although, the Australian government has set-out a five year plan to significantly increase its cybersecurity policies and capabilities, the details are not provided. Also CERT Australia will continue to operate and a hub between the public and private sector. Hence, "information security roles and responsibilities are not thoroughly coordinated and aligned with international roles". This indicates that Australia is currently at level 2.

International cooperation

One of the first major improvement has been the 'ANZUS Treaty to cyberattacks' in 2011 with the United States. According to the joint statement by the United States and Australia "in the event of a cyberattack Australia and the US would consider it together and determine appropriate options to address the threat, reflecting the mutual obligation in Article III of the ANZUS Treaty" (Joint Media Release, 2011). As the previous chapters explain, cyberspace transcends borders and therefore international cooperation is crucial for a strong cyber defense. Australia seeks further and long-term cooperation with the NATO; further indicating a international cooperation awareness. Furthermore, Australia has "committed to developing a comprehensive cyber partnership to address mutual threats and challenges emerging in and from cyberspace" with the United Kingdom and the United States. Finally, Australia will take part in cybersecurity exercises such as the 'Cyber Storm Series' which the United States coordinates. Given this information, Australia is at level 2 (Australian Government Department of Defence, 2013).

Policy development score

The Australian government's strategy currently obtained 7 out 9 points. Cybersecurity is given significantly more prominence in comparison to 2009, however, it is still considered in a conventional way in as much as it is part of the overall military strategy. Furthermore, formal policies and documents are not clearly distributed and defined. Although the responsibility is broadly explained much still needs to be done

2. Austria

The 2012 Austrian National ICT Security Strategy is a comprehensive, detailed and clearly defined strategy paper. Not only is the government aware of the potential threats to its

cyberspace but it aims to raise awareness in all aspect of its society, from the general public to the private sector. Furthermore, the government is developing both reactive and proactive 'cyber incident management'. Additionally, the government is concerned with a cost/effectiveness factor in each of its proposed policies. Finally, a positive factor is the fact that a separate strategy paper is published, thereby treating cybersecurity as a separate phenomenon rather than being part of the other domains of defense such as air, land, space and maritime capabilities (Federal Chancellery Digital Austria, 2012, pp. 4).

Legal foundation

Currently the ICT Consolidation Act contains the most prominent approach for cybersecurity in Austria and the Budapest Convention the most important international document. The Austrian government does not plan to take further action in the short-run. The focus is put on the implementation of the act with regards to the public administration. The reason for this is the fact that cybersecurity should go beyond mere incidents and has to become a part of the day-to-day business. However, legal provisions will be made to include mandatory reports on incidents. If 'cyber anomalies' occur – a term which the Austrian government has not precisely defined – within systems which are not equipped with early warning sensors those networks are still required to report these irregularities. Overall the Security Strategy states that "legal provisions have to be adopted defining the responsibilities and powers of Cyber Situation Centres, their reporting duties and requirements concerning data disclosure" (Federal Chancellery Digital Austria, 2012, pp. 11). Given this Austria receives a score of 2; willingness is present but comprehensive tangible attempts are absent.

Agency responsibility

To date, no separate agency is responsible for cybersecurity. Most of this area is done by CERTs. Nevertheless, the government is highly aware of this and has made it a serious effort to establish a 'Cyber Situation Centre'. The Cyber Centre will operate on a '24 hours a day, 7 days a week' basis thereby ensuring that the monitoring and early warning mechanisms are always active. These two aspects are the main tasks of the Centre. Furthermore, support on request will be created as well in cases where monitoring is not sufficient. For the operationalization of the Centre a cyber partnership will be set-up. Decisions will be 'taken jointly by a Situation Council together with the most important public cybersecurity stakeholders'. What this indicates is a comprehensive approach with the aim of including as many stakeholders as possible. Given that the majority of cyberspace is used by nonpublic

persons and enterprises this is a praiseworthy approach. The central executive will be the 'Chief Cyber Security Officer' who will closely work together with the 'Chief Information Officer in the Federal Republic'. However, the above structure will be used for 'normal operations'. If a crises arises the Public Cyber Crisis Management will take over. As the Report states "Rules and procedures will have to be agreed upon to facilitate cooperation between public and private crisis centres. In the event of a cyber incident with potentially harmful local effects, institutions of the relevant ministries or private entities will be responsible for crisis management in cooperation with CERTs" (Federal Chancellery Digital Austria, 2012, pp. 8-9). The analysis indicates a level 2 score for Austria.

International cooperation

The Austrian Government is aware of the fact that international cooperation is necessary or "a more long-term and international perspective is required in order to stabilize this situation" (pp.3). Austria aims to be a key player in the European Union in the area of cybersecurity. Nevertheless, much more is not discussed and results into 2 out 3 points.

Policy development score

The Austrian government has set-out a detailed and clearly defined action plan. Critical areas have been defined and significant steps have been taken. Although a overarching structure is somewhat lacking, the new strategy clearly defines who is responsible, which actions should be taken in case of an incident and cost-benefit analyses are performed. A significant level of maturity has been reached. However, routines test are not performed and although the government aims to make integrate ICT security in both public and nonpublic organizations, this is not yet the case. Therefore, the Austrian strategy currently receives a score of 6 points in total.

3. Belgium

Legal foundation

Belgium aims to develop a clear legal framework to balance privacy and security. The Belgium cybersecurity policy uses existing national and international provisions as the starting point for the continued development of its cybersecurity strategy. However, for its national strategy the government aims to increase jurisdiction and the legal basis for a more long-term and stronger framework. The competences of the security services, police and justice departments will have to be adjusted to respond to the changing threats to its

cyberspace (Belgian Cyber Security Strategy paper, 2012). Therefore, not much has been developed next to the Budapest Convention. As Belgium is currently reviewing existing legislation, the implementation level has been reached.

Agency responsibility

Belgium established a Centre for Cyber Security. (CCSB). The CCSB falls under the responsibility of the Belgian First Minister. The Centre will be the central coordination organ, which will cooperate will other departments and agencies such as CERT Belgium (CERT.be) and the Departments of Foreign Affairs and Justice amongst others. BelNIS will be the discussion platform in which the coordination between the different departments will be arranged. BelNIS will be chaired by the director of the CCSB. However, every department will operate autonomously and will not be given a mandate or resources; indicating a level 1 situation (Belgian Cyber Security Strategy paper, 2012).

International cooperation

Belgium wants to create its own cybersecurity capacity given that international support in case of a cyber incident is not always evident. Therefore, although international cooperation is sought, the goal is to increase national capabilities first. The reason is that the government expects to increase international cooperation after it has developed its national cyber expertise first. Finally, the Belgium government will continue cooperating with other CERTs, both on a European and International scale – Belgium is internationally active, yet not to its fullest potential and results into 2 out 3 points (Belgian Cyber Security Strategy paper, 2012).

Policy development score

The Belgian Strategy paper and developments clearly express the current plans of the government. The roles have been clearly defined and all major facilities and operations are broadly covered. Additionally, the policies define who is responsible for which tasks, when and how measures must be taken. Nevertheless, initial testing is only limited and hence the Belgian government is still in the implementation phase. Therefore, Belgium has currently 5 out of 9 points

4. Canada

Legal foundation

Canada developed an action plan 2010-2015 for its Cyber Security Strategy in which it

expressed the concern with transnational cybercrimes and feels a need to develop its 'investigative powers and tools' for its law enforcement authorities, a big part of these powers is a new legislative authority. The Canadian government has passed legislation against identity theft and will continue to pass legislation for other cyber related crimes. The Strategy paper addresses criminalizing sexual exploitation of children with the use of a computer; requiring internet providers to 'maintain intercept capable systems' and to provide the police and other law enforcement agencies with 'basic customer identification data'. With regards to military capabilities of cyberspace the Canadian government want to cooperate with other countries for an international effort against the threats for the Canadian government and industry (Canada's Cyber Security Strategy, 2010). Canada was involved in the drafting of the Budapest Convention however, has not ratified it. Therefore, Canada cannot be regarded to be at the integration stage up until this point.

Agency responsibility

The strategy paper mentions that the "Royal Canadian Mounted Police will be given resources to establish a centralized Integrated Cyber Crime Fusion Centre". The new centre will cooperate with the newly established 'Canadian Cyber Incident Response Centre' – the primary national cyber centre - for the protection of the national infrastructure and attacks on the Government and its agencies. Additionally, 'Public Safety Canada' will continue to increase awareness under the general public about the potential threats and measures to protect themselves. Overall, the Canadian Security Intelligence Service is responsible for 'domestic and international threats to the security of Canada' and the Royal Canadian Mounted Police will analyze 'domestic and international criminal acts against the Canadian Networks and critical information structure'. Finally, the Treasury Board Secretariat will continue to increase support for improved cyber capabilities and management across the Government 'through the development of policies, standards and assessment tools' (Canada's Cyber Security Strategy, 2010).

International cooperation

Canada focuses on cooperation with Australia, the United Kingdom and the United States. The goal is to increase collective security and to have similar 'domestic cyber regimes'. Additionally, engagement with international organizations such as the NATO, the UN and the Council of Europe – whose 'Convention on Cybercrime' Canada is a party to – is stimulated (Canada's Cyber Security Strategy, 2010). As a result of its active international engagement

Canada is currently at the integration stage.

Policy development score

Roles and responsibilities in the area of cybersecurity are assigned and cover all major areas. Therefore, when, how and who to respond is made clear to the government employees and officials. Overall, Canada has 7 out of 9 points; the plans are rather elaborate and the issue is dealt with in a separate strategy paper, however, self-assessment and continuous testing appears to be absent.

5. Czech Republic

Legal foundation

In addition to the Budapest Convention of 2001, the Czech government has drafted an Act on Cyber Security (2014) in which it clearly determines who is responsible, which measures should be taken in case of an incident and the allowed response period. Furthermore, the National Security Authority (NSA) has identified in the specialized law the responsibilities of the National Centre for Cybernetic Security (NCCS). Overall, both public, private, and international responsibilities and obligations are listed. The government actively participates in the drafting of international agreements and laws with organizations such as the EU, the NATO and others; translating into a level 2 – implementation stage (Strategy of the Czech Republic in the field of cybernetic security for 2012-2015).

Agency responsibility

Under decisions no. 781 (Czech Republic, 2013) the government states that the NSA is responsible for the area of cybersecurity. The Czech Republic established the Council For Cybernetic Security which is important for 'the inter-ministerial coordination'; in essence the Council will review and distribute works from experts and other agencies. Within the NSA the NCCS will be responsible for the cooperation between the different state bodies and for the improvement of coordination and implementation of counter-measures'. Additionally, CERT is envisioned to be part of the NCCS. Thus, level 2 has been reached; Given that the responsibility structure is currently reviewed (Czech Republic, 2011).

International cooperation

The Czech Republic is highly aware of the need for international coordination and hence actively participates with the EU, NATO and other international organization for the

establishment of norms, standards and legislation in the field of cybersecurity. The recommendation and proposal of the NSA shall cooperate with the European Network and Information Security Agency (ENISA) and take into account the NATO Policy on Cyber Defense, as well as other EU proposals and strategies. Despite the awareness, the Czech Republic can be more considered as a participants rather than an agenda setter indicating a level 2 situation (Czech Republic, 2011).

Policy development score

The Czech republic has drafted a clear and comprehensive act on cybersecurity. Furthermore, the responsibilities, roles and action plans are clearly defined. The agencies responsible have suitable guidelines and international cooperation is actively sought. Nevertheless, as ICT security has not developed into as an integrated practice and the continuous review of policies is not possible before the legislation is properly adopted the current score is 6.

6. Denmark

Legal foundation

The Danish government did not publish a separate cyber strategy document. Rather the government incorporated cybersecurity in the 'Danish Defense Agreement 2013-2017' has the perspective that cyber threats are newly emerging together with risks in for example the Arctic. Throughout the Defense Agreement the Arctic and cybersecurity are mostly discussed under the same header (Danish Government, 2012). Nevertheless, Denmark was one of the first countries to ratify the Council of Europe's Convention on Cybercrime or Budapest Convention of 2001; indicating a willingness to cooperate and hence a level 2 position.

Agency responsibility

The Danish government agreed to establish 'a Centre for Cyber Security' under the Ministry of Defense. In addition, the government has reserved around 35 million Danish Mark per year for further development of the Centre. Even larger amounts have been reserved for the development of a Computer Networks Operation (CNO). The priority of the CNO is increase 'defensive and offensive military operations in cyberspace' (Danish Government, 2012). These commitments indicate that Denmark is currently implementing a new cybersecurity regime or framework.

International cooperation

The Danish government seeks cooperation with allies and international organizations such as the NATO and the EU and will actively participate during meetings and conferences. As a result of this Denmark is at level 2 with regards to international cooperation (Danish Government, 2012).

Policy development score

The Danish government appears to be somewhat behind in the area of cybersecurity. Although military capabilities are developed and a Centre for Cyber Security is supported by the government, the overall tendency is to view 'cyber' as part of traditional military areas. Furthermore, the Danish government has not extensively developed legislation nor clearly assigned roles and responsibilities of specific incidents and operations. Therefore, the Danish cybersecurity policy development process receives 6 out of a possible 9 points. .

7. Estonia

Legal foundation

Estonia is developing a far-reaching and robust legal framework for the field of cybersecurity, beyond the ratified Budapest Convention. The 2008 Cyber Security Strategy addresses the following areas; "development of legal definitions for cybersecurity and cyber crime; development and implementation of legislation to ensure cybersecurity, including the introduction of compulsory security measures and standards in critical infrastructure companies and the establishment of minimum information security requirements for all information systems; improvement of existing legislation with a view to ensuring cybersecurity; drafting of new legislation to cover new areas or threats; launching of initiatives in international law-making". Furthermore, new legislation and amendments were made in the penal code, Electronic Communications Act, Personal Data Protection Act, Public Information Act, and the Information Society Services Act. This comprehensive revision of the legal framework makes it possible to classify Estonia as level 3 country (Ministry of Defence Estonia, 2008).

Agency responsibility

The NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE) is established in Estonia. Furthermore, the government agencies operate trough a 'three level baseline security system (ISKE). As a result "a multilevel system of cybersecurity measures will be employed for the protection of the critical information infrastructure, development and implementation

of a system of security measures, strengthening of organizational co-operation" (Ministry of Defence Estonia, 2008, pp. 27-28). The structure, although explicit, can benefit from routine tests and more cooperation. Therefore, currently Estonia is not at the integration level.

International cooperation

Estonia actively cooperates and promotes IT security on a national and international level. Additionally, Estonia cooperates with the UN, NATO, the EU, the Council of Europe, the OECD and OSCE. As a result, many multi-lateral and bi-lateral agreements have been reached. Furthermore, Estonia seeks cooperation with multinationals and international IT companies. The aim is to develop a comprehensive international legal framework as this is still absent today (Ministry of Defence Estonia, 2008).

Policy development score

Estonia is developing a strong legal framework which addresses all the different aspect of cyberspace and the potential risks to it. Furthermore, a large array of stakeholders are included and consulted with the CCDCOE as the overarching authority. The stakeholders include experts, scholars and risk analysts. Additionally, Estonia is active in international cooperation and the development of new policies. However, there is not yet a culture of integrated ICT security and therefore Estonia receives 8 points.

8. Finland

Legal foundation

In 2007 Finland ratified the Budapest Convention but furthermore the government of Finland is not in favor of a strict legal framework. The 2013 Cyber Security Strategy states that "Cyber security is not meant to be a legal concept the adoption of which would lead to granting new competences to authorities or other official bodies" (Government of Finland, 2013, pp. 2). Therefore, no new legislation or amendments are proposed in the latest strategy paper. Furthermore, the government does not want 'regulations concerning the competences of authorities'. Nevertheless, the government is concerned with providing "competent authorities and other actors with the sufficient means and powers through legislation to implement cyber defences for the functions vital to society and, especially, the security of the state". In addition, possible legal restrictions, both national and international "that impede the obtainability, disclosure and exchange of information useful for effective cyber defence

purposes, will be taken under review" (Government of Finland, 2013, pp.10). Overall, the government will take privacy and data protection into account but wants a less restrictions on the authorities as possible; indicating level 2.

Agency responsibility

On January 1, 2014 the government establish the National Cyber Security Centre Finland (NCSC-FI) which falls under the authority of the Finnish Communications Regulatory Authority (FICORA). Furthermore, "a strategic cyber security centre of excellence will be established under the existing ICT-SHOK (TIVIT). It will provide an opportunity for top research teams and companies who utilise the results to engage in effective mutual cooperation over the long term. The centre of excellence will facilitate the conditions for the establishment of a robust national cyber security cluster" (Government of Finland, 2013, pp. 10).

International cooperation

Finland will cooperate with international organizations such as the EU, NATO, UN, OECD and OSCE. The goal is to increase the national cybersecurity quality with the use of international exercises and the exchange of information.

Policy development score

Finland is currently at the implementation level for all three dimensions. Indicating a score of 6 out 9. Although a Cyber Centre is developed and cooperation is sought, the separate cyber strategy paper appears to lack a clear direction and only the government only very recently started to make progress. Furthermore, although Finland has made a threat scenario analysis in the 2010 national defense paper, the appropriate (counter) measures seem to be less developed. The Finnish government will significantly contribute from international experience and information given that the assignment of roles, procedures and legislation require improvements.

9. France

In the latest strategy paper, the 2013 White Paper on Defense and National Security, Cyber risks are listed next to other possible future threat and the government expresses the increased awareness of possible dangers in the area of cybersecurity.

Legal foundation

In France's information systems defense and security strategy paper (2011) adapting French legislation is part of its 7 point plan. Therefore, the government is concerned with the adaptation and implementation of new laws and regulations to increase its cybersecurity capabilities. Therefore, if new technologies or incidents arise the government will take appropriate action. The only tangible reform currently enacted is the 'enforcement of the General Security Framework (RGS)'. The RGS "will allow public authorities to significantly raise the protection levels of their information systems, particularly in their relations with users". Overall, very few details are mentioned and hence it is questionable how much has been done to date, resulting into a classification as level 1 (French Network and Information Security Agency, 2011).

Agency responsibility

The French government is investigating the creation of a cyber defense research centre together with stakeholders from the IT industry. The centre's main goal would be to develop security methods, software and stimulate scientific research. In 2009 the French Network and Information Security Agency (ANSSI) was created and since 2010 is responsible for the 'defense of information systems'. Given the creation of the ANSSI and subsequent agencies and the continued execution of the 7 point plan, France is currently at the implementation stage (French Network and Information Security Agency, 2011)

International cooperation

The 7 point plan in the 2011 strategy paper mentions international cooperation as one of the main development areas. The paper states that "France is building a highly select circle of trustworthy partners with whom indepth operational exchanges will be held" (French Network and Information Security Agency, 2011, pp. 18). Additionally, the government wants to work together with other international partners for information sharing and seek 'partners to fight cybercrime'.

Policy development score

The legal framework of France for its cybersecurity is somewhat limited. Furthermore, there appears to be no clear division in tasks, responsibilities, and reactionary methods. In addition, the vulnerability of all areas is not assessed, rather France seeks to fight cybercrime. Even though this is necessary, cyber crime is only one risk out of many. Thus, France has

developed action points and is still in the process of execution. Therefore, France has an overall score of 5 points.

10. Germany

Legal foundation

Currently no new legislation is proposed, although improvement are considered. Germany does have a Critical Infrastructure Plan (CIP) for which legal provisions and commitments are examined in cooperation with the National Cyber Security Council, as well as having ratified the Budapest Convention. Germany can be considered to have understood civil liberties, international obligations, and hence is at level 2 (Federal Ministry of Interior Germany, 2011).

Agency responsibility

A National Cyber Response Centre was set up in 2011. The Centre works together with the Federal Office for the Protection of the Constitution (BfV) and the Federal Office of Civil Protection and Disaster Assistance (BBK), and reports to the Federal Office for Information Security (BSI). All relevant authorities in for the protection of cyberspace and its different aspects cooperate with the Centre. The recommendations developed by the Centre are distributed to the National Cyber Security Council, which is headed by the Federal Government Commissioner for Information Technology. Germany further plans to have effectiveness analyses. Therefore, the current situation is level 3 (Federal Ministry of Interior Germany, 2011).

International cooperation

Germany supports and stimulates development of the ENISA at the EU. Furthermore, any national developments will take into account international organizations such as the UN, OSCE, Council of Europe, OECD and NATO. Furthermore, Germany is in favor of a international cyber code ‘for state conduct in cyberspace’. Finally, in cooperation with NATO Germany attempts to create ‘uniform security standards’ and urges the organization to do everything possible for the protection of cyberspace. This makes Germany a leader in the field of international cooperation for the protection of cyberspace (Federal Ministry of Interior Germany, 2011).

Policy development score

Germany has 7 points on the Policy development scale. The government has significantly developed its cyber policies and created strong agencies. Furthermore, a wide range of stakeholders are included and the division of tasks is clear. Additionally, international cooperation is highly valued and stimulated. However, the testing and corrective measures still require more attention.

11. Hungary

Legal foundation

Next to being one of the first signatories of the Budapest Convention, Hungary also initiated the 2013 Act on Electronic Information Security of Central and Local Government Agencies. The Act is very detailed and amongst other clearly defines potential threats, actors and reactionary measures. Therefore, the integration level has been reached (Government of Hungary, 2012; Government of Hungary, 2013).

Agency responsibility

The Government Incident Management Centre has the main responsibility for cybersecurity and works together with the Sectoral Incident Management Centers for specific sectors. Furthermore, Hungary aims to establish ‘cyber security centers of excellence’, in which the cooperation with universities and scientists is fostered for the improvement of research and development. Overall, the Prime Minister’s Office coordinates the individual government agencies which are all responsible for ‘free and secure use of the cyberspace’. Thus although an overarching structure exists, a more integrated and threat scenario analysis is absence; point out a level 1 situation (Government of Hungary, 2013).

International cooperation

Hungary sees a strong role for the NATO and the EU and is an active participant in the organizations. Furthermore, the OSCE, UN, Council of Europe and other international organizations are mentioned as valuable cooperation platforms. Finally, Hungary attempts to foster and increase cooperation with regional Eastern and Central European countries and organizations. Although a active participant, the lack of clear action points results into 2 out 3 points (Government of Hungary, 2013).

Policy development score

Hungary has made impressive progress with its 2013 Cyber Security Strategy. International and regional cooperation is sought and stimulated. Furthermore, a national action plan and prospect of centers of excellence are being developed. Additionally, the 2013 Act clearly defines threats, actors and areas. However, as the different government organizations are individually responsible, the coordination seems to be less developed and the Incident Centre is only recently established. Therefore, Hungary has a 6, with some issues being integrated and others still requiring review and tangible efforts.

12. Italy

Legal foundation

The 2013 'National Strategic Framework for Cyberspace Security' is a significant step forward. Furthermore, as the Strategy Paper points out, the responsibility and methods of the national CERT are defined in Article 16 of the Legislative Decree no. 259/2013. Additionally, the Committee for the Security of the Republic (CISR) can propose legislative initiatives. However, a comprehensive understanding and management of all aspects is not visible. Consequently, Italy has reached the implementation level will need more time before the CISR can address every specific issue and sector (Presidency of the council of ministers, 2013)

Agency responsibility

The National Anti-crime Computer Centre for the Protection of Critical Infrastructure (CNAIPIC) is responsible for cyberattacks of 'strategic assets' which falls under the authority of the Postal and Communication Police. Whereas CERT is responsible for public-private cooperation in the area of cybersecurity and different CERT branches are responsible for different government departments. The division of tasks exposes a lack of integrated structure and clear leadership (Presidency of the council of ministers, 2013).

International cooperation

Italy participates in international organizations which it is a member to. Furthermore, cooperation with allies is attempted. The National Framework states that Italy wants to "participate actively in all relevant international forums and working groups" (Presidency of the council of ministers, 2013, pp. 22 Thus Italy, is an active member, yet not a forerunner.

Policy development score

Italy has made it explicit which agency is responsible in which area. Furthermore, international partnerships, cooperation and participation in exercises is actively pursuit. However, a risk-benefit analysis, threat scenarios and tests appear to be absent. Although the topic is treated in a separate strategy paper, indicating the awareness and importance, Italy is currently the implementation level in all three dimensions and hence has 6 out of 9 points.

13. Latvia

Legal foundation

Latvia has not published a Cyber Security Strategy paper. However, the law on the Security of Information Technologies identifies responsibilities, actors, and different possible risk situations and is the main provision next to EU directives and the Budapest Convention. Therefore, Latvia has reached the implementation level (Government of Latvia, 2010).

Agency responsibility

The main responsibility falls under the Information Technologies Security Incidents Response Institution which 'shall promote the security of information technologies' for Latvia. However, if a dangers incident occurs the responsibility can be transferred to the national armed forces. Additionally, national and local authorities are required to appoint a responsible person for their respective IT sectors. These responsible persons have to examine, propose changes and identify threats on a yearly basis (Government of Latvia, 2010).

International cooperation

The Response Institution shall seek international cooperation and can report dangers and incidents to EU institutions and agencies. Furthermore, international knowledge and information sharing should be promoted; indicating passive membership (Government of Latvia, 2010).

Policy development score

Latvia is currently still developing their cyber framework. Although information sharing, research and development is strongly supported an effective response mechanism appears to be absent. Furthermore, international cooperation should be more strongly sought. Finally,
Therefore although testing is performed – a level 3 requirement – not all security controls are

sufficiently supported and the National Cyber Security Strategy itself should be more clearly defined, hence Latvia currently has a total of 5 points.

14. Lithuania

Legal foundation

Although Lithuania ratified the Budapest Convention, this does not cover everything. Additionally, national legislation is highly fragmented and very limited. The stakeholders are not clearly defined, neither are the areas, threats and responsible actors. Furthermore, a strategy or framework to respond to cyber incidents is virtually absent (Government of the Republic of Lithuania, 2011).

Agency responsibility

Although CERT Lithuania (CERT-LT) is operational, internet provides and other digital and communications service providers are not legally required to report incidents. The only agencies currently responsible for cyberattacks is the Lithuanian Internet Traffic Exchange node and can be used in the future for more effective cyber protection (Government of the Republic of Lithuania, 2011).

International cooperation

One of the main objectives of the Lithuanian government is to develop international cooperation, however, to date not much has been accomplished (Government of the Republic of Lithuania, 2011).

Policy development score

Lithuania is aware of the threats to its cyberspace. However, very little has been accomplished to date. The actors, responsibilities and protocols are not defined and reactionary measures are absent. Given the very undeveloped set of policies Lithuania is currently at level 1 in all dimensions and has a total score of 3 out of 9.

15. The Netherlands

Legal foundation

The Netherlands published the second National Cyber Strategy paper in 2013 and the Cyber Defense Strategy in 2012. The Budapest Convention serves as a guiding principle with

national legislation being harmonized in accordance with this and other international agreement. There is significant attention paid to ‘updating and strengthening (international) criminal legislation, including the Computer Crime Act III – the new version which will be published in 2014 (National Coordinator for Security and Counterterrorism The Netherlands, 2013). As this is still a proposal and not a practice, the Netherlands is at the implementation stage.

Agency responsibility

The National Cyber Security Centre (NCSC) is the main organization for both the public and the private sector. The NCSC will additionally serve as a CERT and Security Operations Centre (SOC). The Defense organizations participates in the Cyber Centre and in the Cyber Security Council. Furthermore, The Joint Information Command – operational since 2013 – develops and implements ‘adequate and high-quality security measures and ensure the protection of all networks and systems’. Finally, the Defense Computer Emergency Response Team (DefCERT) are has a monitoring function and uses ‘threat levels’ and will become part of the Joint Information Command which in turn cooperates with the Defense Intelligence and Security Service (Ministry of Defence The Netherlands, 2012; National Coordinator for Security and Counterterrorism The Netherlands, 2013).

International cooperation

The Netherlands wants to extent cooperation with Europol and the EU (National Coordinator for Security and Counterterrorism The Netherlands, 2013). Both the NCSC and the Joint Information Command work together with NATO, other CERTs and other international organizations. The Netherlands is an active member without any tangible international proposals and hence is at level 2.

Policy development score

The main actors, areas and threat are made clear and continuously updated. The division of responsibilities is clear and the second strategy paper shows the significant progress which the Netherlands has made. All threat areas are mapped and appropriate agencies, actors and measures are identified. However, the Netherlands still needs to work out which capabilities the defense organization will have at its disposal. The Netherlands has an overall score of 6; and is as the title of the strategy indicates moving from ‘awareness to capability’.

16. New Zealand

Legal foundation

New Zealand is considering to incorporate the standards of the Budapest Convention. Furthermore, in partnership with internal security partners the government is reviewing its legal framework in an attempt to better prepare for the possible threats for its cyberspace – preparing policies and hence level 1 (New Zealand Government, 2011).

Agency responsibility

The government has established the National Cyber Security Centre under the Governance of the Communications Security Bureau. The Centre has absorbed the Centre for Critical Infrastructure Protection (CCIP). CERT New Zealand is currently under examination – to see if renewal is necessary (New Zealand Government, 2011).

International cooperation

The Government of New Zealand seeks cooperation with its international security partners. Participation in international forums is important and the government is aware of the need. However, currently little has been accomplished (New Zealand Government, 2011).

Policy development score

The New Zealand cybersecurity policy is very much in its infancy and can be considered to be in the 'policy stage' for all dimensions, indicating an overall 3 points in total.

17. Norway

Legal foundation

Norway sees a need to develop its legislative framework for the prevention and reaction to cyber threats and attacks. There is a problem given that there are insufficient law enforcement officials for the investigation of cyber incidents. Therefore, the government attempts to clarify which legal requirements apply to government organizations and ministries. This is highly necessary because the current conviction rate is very low. However, the Norwegian Data Protection Authority – which supervises the relevant regulations and laws – has "developed a number of guidelines on information security and provides guidance on compliance with legislated requirements" (Norwegian Ministries, 2012, pp. 30). As Norway is currently at level 2 this means that policies and guidelines are proposed and are expected to significantly

improve the cybersecurity framework of Norway.

Agency responsibility

The responsibility for information security in Norway is divided. Overall, the government has the ultimate responsibility, and the ministries are expected to include all stakeholders and actors within implementation of the Norwegian strategy priorities. Furthermore, the persons in charge of businesses, municipalities and counties are responsible cybersecurity effort in their respective sectors. In more detail "the Centre for Information Security (NorSIS), the Business Security Council, the Norwegian Data Protection Authority, the Post and Telecommunications Authority and the Media Authority (pp. 23)" are the leaders in the different sectors. The Norwegian National Security Authority (NSM) is the central organ and is mostly concerned with critical infrastructure and information protection, with CERT Norway (NorCERT) being responsible for the notification of incidents (Norwegian Ministries, 2012).

International cooperation

NorCERT cooperates with response teams of other countries and international organizations. Especially a Nordic CERT collaboration is important in this respect. In general, the government stimulates Norwegian collaboration in international forums, both from the public and private sector, with a special emphasis on the research and university community. Norway can be classified as an active member and strives to improve its collaboration with other countries (Norwegian Ministries, 2012).

Policy development score

Norway is developing a legal framework and increasing its knowledge and countermeasures. However, Norway is at the implementation phase – 6 out 9 points – with international cooperation being fostered but effective mechanisms and initial testing still mostly absent.

18. Poland

Legal foundation

The main legislative act is the Act of 5 August 2010 on the protection of classified information (OJ No. 182, item 1228). The Polish Strategy discusses that "the achievement of the strategic objective is accomplished by creating a legal and organizational framework and a

system for effective coordination and exchange of information between the users of CRP" (Government of the Republic of Poland, 2013, pp. 6). The report continues and states that "it is necessary to review the existing regulations with a view to the preparation of solutions aimed at increasing the sense of security, not only of government institutions, but of all the users of cyberspace" (pp. 6-7). The report talks about a need for review, thereby indicating an aim to improve the structure, as concrete proposals appear absent Poland is currently at the policy level (Government of the Republic of Poland, 2013).

Agency responsibility

The 'Governmental Computer Security Incident Response Team' (CERT.GOV.PL) is the most important response team for both the civil sector and public administration. For the military sector the primary organization is the 'Departmental Centre for Security Management of ICT Networks and Services'. All agencies and government administration departments are required to submit a risk assessment report to the minister responsible. The Prime Minister will assign a special team which is concerned with coordination and implementation of cybersecurity recommendations. Additional, under government Decision no.1/2012 the "chairman of the Committee of the Council of Ministers for the Digitization" can appoint a 'task force for the protection of government portals' to support the above mentioned team. The Minister of National Defense, the Head of the Internal Security Agency and the Minister responsible for information protection will cooperate in setting guidelines and to ensure consistency in the different units and departments. Thus, the structure is clear and routine risk assessment reports are scheduled. The division of tasks is clear and the government plans to have self-assessment procedures, showing an integrated level of agency responsibility (Government of the Republic of Poland, 2013).

International cooperation

The Polish government will improve international and national information exchange. International cooperation is perceived as crucial for the protection of cyberspace. Therefore, the government will be active and collaborate with non-governmental and international organizations to improve their cybersecurity framework (Government of the Republic of Poland, 2013).

Policy development score

The cybersecurity policy of the Polish government is being developed. Whereas, legal

foundation is at level 1, agency responsibility is at level 3, and international cooperation at level 2. Although much has been achieved, the actual performance is not complete. The government is working hard to improve its data and information protection and receives an overall score of 6.

19. Slovakia

Legal foundation

The Slovakian government regards 'EU directives, OECD recommendations, and key international norms and standards' as crucial for a strong legal framework. The government has taken several legislative steps and introduced regulations in accordance with the international agreements and standards for the improvement of their own legal framework. The regulations range from the public administrations usage of information systems to amendments in the Penal Code. Furthermore, the government has been an active participant in international conventions such as the Council of Europe and the OSCE. However, the attempts primarily stem from the willingness to cooperate with international regulations and do not reflect a comprehensive account of all legal requirements for cybersecurity; a level 1 situation (Government of the Slovak Republic, 2008).

Agency responsibility

The formation of a specialized CERT unit – the 'Computer Security Incident Response Team Slovakia' (CSIRT.SK) was an important step for stronger cybersecurity framework. A three-tier structure is currently active in Slovakia. The primary body the government as it sets approves any proposals or strategies. Secondly, a central government body – which includes the relevant ministers for the area of cybersecurity. The third tier are more specialized and specific government authorities and committees. However, the government is reforming the management structure to have a more efficient and effective organization. The process should cumulate in the formation of the National Information Security Authority of the Slovak Republic (NISA) (Government of the Slovak Republic, 2008). A structure is present, however, it requires significant reforms which has been set in motion. For the current classification, Slovakia is still at the policy level.

International cooperation

The Slovakian government is represented in many international organizations such as the

ENISE and working groups of the EU, OECD and NATO (Government of the Slovak Republic, 2008). However, as a result of the limited capability expertise and resources Slovakia is in most organizations an observer and not an active member.

Policy development score

Slovakia is a difficult case, although the government has proposed policies and has implemented a organizations structure much still needs to be changed. As stated above, the government is actively reforming its structure, organization and legislation. Furthermore, as Slovakia is mostly an observer rather than an active member at international forums, Slovakia can be classified as level 1 in all dimensions, and has an total score of 3.

20. Spain

Legal foundation

Spain has some legislation, however, this is fragmented and does not reflect a common strategy. The legislation is dispersed between the different agencies and policy areas. Therefore, the government is developing a common strategy and a 'legislative framework to support National Cyber Security'. For this aim, the government will provide necessary resources and capabilities (Spanish Cyber Security Institute, 2013). The efforts of the government in conjunction of the ratification of the Budapest Convention indicates that Spain can be classified as level 2.

Agency responsibility

The National Security Council is the main body on which the Prime Minister of Spain relies. Secondly, the specialized committees are important for specific areas (National). The Spanish government regards cybersecurity as a shared responsibility of all ministries and both national and international. In more detail, the powers are distributed amongst regional and national institutions; the National Institute of Technology and Communication and its CERT (INTECO-CERT), National Cryptology Centre has a response team (CCN-CERT) – which falls under the National Intelligence Centre (CNI), National Centre for Critical Infrastructure Protection (CNPIC), Computer Crime Unit of the Guardia Civil, Spanish Data Protection Agency (AEPD), and the regional CERTs of Catalonia, Andalusia and Valencia. Finally, the Spanish Armed Forces are led by the Chief of Staff of National Defense and are responsible

for their sector (Spanish Cyber Security Institute, 2013). The cybersecurity structure in Spain is highly fragmented and can improve with a more centralized command centre.

International cooperation

The Spanish government wants exercises 'from time to time' both nationally and within the NATO, EU and other international organizations. Furthermore, the national CERT works together with other CERTs on an international scale and 'collaboration agreements have been signed'. Finally, multilateral and bilateral agreements are according to the Spanish government necessary for the protection of cyberspace. As a result, Spain is an active member in international forums such as the OECD, NATO, EU, UN, Interpol and Europol (Spanish Cyber Security Institute, 2013).

Policy development score

The government is developing a comprehensive, common and effective legal framework for the protection of its cyberspace. All tasks, responsibilities and actors are clearly defined. However, some effective overarching authority is not visible and the strategy is not specific and detailed enough. Furthermore, test are planned yet not carried out, and international leadership capabilities are absent. Therefore, Spain currently has 5 points on the development scale.

21. Turkey

Legal foundation

In 2013 the Turkish government examined domestic and international regulations for the formulation of a complete legal framework; thereby ensuring that the new national legislative acts were in accordance with international agreements. The government reviewed and updated "current main regulations (laws) in a way to cover the subjects that need to be handled in the area of cybersecurity, and completing the primary legislative activities that would meet the needs for new regulations, and submitting them to the Cyber Security Council" (Ministry of Transport, Maritime Affairs and Communications Turkey, 2013, pp. 24). On a ongoing basis 'secondary legislative activities' are being revisited. Turkey has not ratified the Budapest Convention and has not taken into account all privacy and civil liberties obligations. Therefore, the legal foundation is still at level 1.

Agency responsibility

In 2013 the Cyber Security Council started operating as a result of the 'National Cyber Security Strategy 2013-2014 Action Plan. This is a comprehensive, wide-ranging plan which determines the main actors, sectors and responsibilities. Furthermore, the National Cyber Incident Response team (USOM) and 'Teams for Responding to Cyber Incidents against Sectoral and Public Entities (SOME)' were established. Furthermore, cybersecurity exercises are scheduled once every two years, starting in 2013 (Ministry of Transport, Maritime Affairs and Communications Turkey, 2013.)

International cooperation

As is the case with most countries, Turkey fosters international 'cooperation and information sharing'. The USOM serves as 'the national contact point' and will cooperate with international counterparts. Finally, Turkey sees it as a goal to take part in international conferences and seminars in the area of cybersecurity. Turkey can, however, not be considered as a significantly active participant (Ministry of Transport, Maritime Affairs and Communications Turkey, 2013).

Policy development score

Turkey has made significant steps in their cybersecurity policies. Test are scheduled and will be carried out as planned, task are divided and stakeholders determined. Nevertheless, the legal foundation requires significant improvement and international cooperation should more actively be sought. Turkey has obtained 4 out 9 points.

22. United Kingdom

Legal foundation

The UK puts an emphasis on promoting their 'sounds domestic legal framework and regulatory environment' internationally. According to the strategy paper, the UK government want all countries to have a proper legal basis as this is crucial to respond to cyber threats and risks. To extent their legal framework with "the network of law enforcement contact points know as the 24/7 Network" (Cabinet Office United Kingdom, 2011, pp. 9). However, the government is aware of the development taking place in the digital domain and therefore will review existing laws and regulations on a continuing basis. This indicates that the UK is at level 3; integration.

Agency responsibility

In 2010 a 'four-year National Cyber Security Program (NCSP)' was initiated. The Office of Cyber Security and Information Assurance manages the NCSP and falls under the authority of the Minister for the Cabinet Office. Furthermore, funds are supported to the intelligence services and other relevant agencies and departments. The government response team (GovCertUK). An important aspect is the yearly routine tests to ensure that all information and services are up-to-date. For defense purposes a Global Operations and Security Control Centre is opened. Additionally "A second Joint Cyber Unit embedded within the centre at Corsham will develop and use a range of new techniques, including proactive measures, to disrupt threats to our information security" (Cabinet Office United Kingdom, 2011, pp. 27). Finally, the 'Centre for the Protection of National Infrastructure' has a response team (CSIRTUK) and is crucial in the protection against threats in this area, for both private businesses and government agencies responsible.

International cooperation

The UK collaborates with the Commonwealth, the Council of Europe, the OSCE, the UN, and the EU. The 2011 London Conference on Cyberspace shows the effort of the UK concerning cybersecurity. The Budapest Convention is ratified and the UK strives to "establish internationally-agree 'rules of the road' on the use of cyberspace" (Cabinet Office United Kingdom, 2011 pp. 27). Finally, on EU level the UK wants to review provisions such as the EU Data Protection Directive and the planned "Strategy on Information Security".

Policy development score

The UK is very active in the field of cybersecurity. Many international attempts are made to create a more secure global cyberspace. Additionally, the protocols, actors and risk areas are made clear. The only improvement for the UK would be to more rigorously and frequently have audits, test, and risk analyses. The UK has obtained a total score of 8 out 9.

23. United States

Legal foundation

The USA, despite not being a member country of the Council of Europe, has ratified the Budapest Convention. Furthermore, the US government has further implemented a wide array of laws and amendments as can be seen in appendix I.

Agency responsibility

United States has a Computer Emergency Readiness Team (US-CERT), similar to those of the other countries analyzed. The division of tasks is made clear as US-CERT is more concerned with public-private security. Furthermore, the United States has provided the 'Strategic Command' (USSTRATCOM), the 'other Combatant Commands', and the 'Military Departments' with a specific mandate and these agencies are assigned with 'cyberspace missions'. Furthermore, the United States Cyber Command (USCYBERCOM) is established 'as a sub-unified command of USSTRATCOM'. All fall under the Department of Defense and the Secretary of Defense (United States of America, 2009; United States of America, 2011).

International cooperation

The US cyber policy is far more concerned with military security. The 2011 strategy paper addressed issues such as cyberterrorism, cyberwarfare and other international criminal attempts. The US seeks international cooperation to combat these international threats. Furthermore, "the United States is committed to tracking and disrupting terrorist and cybercrime finance networks through technical tools and international cooperations frameworks such as the Financial Action Task Force" (United States of America, 2011, pp. 20). The US is actively supporting multi- and bilateral agreements and has made it a priority to support other countries. Finally, the US is one of the few countries in this analysis which mentions Africa, APEC, AEAN, and the OAS as countries they aid in training (United States of America, 2009).

Policy development score

The United States has initiated multiple laws and made amendments to compliment its cybersecurity framework. The national defense cyber security is made clear and explicit; all relevant actors and agencies have been indentified and accountability is apparent. Furthermore the comprehensive international cooperation attempts and results have resulted into a maximum score of 3 out of 3 for the international cooperation dimension. Overall, the United States has obtained the maximum of 9 out 9 points and can be regarded to be at the integration stage for all three dimensions.

Appendix H - Budapest Convention

Country	Signature	Ratification
1. Australia	-	2012
2. Austria	2001	2012
3. Belgium	2001	2012
4. Canada	2001	-
5. Czech Republic	2005	2013
6. Denmark	2003	2005
7. Estonia	2001	2003
8. Finland	2001	2007
9. France	2001	2006
10. Germany	2001	2009
11. Hungary	2001	2003
12. Italy	2001	2008
13. Latvia	2004	2007
14. Lithuania	2003	2004
15. The Netherlands	2001	2006
16. New Zealand	Considering	-
17. Norway	2001	2006
18. Poland	2001	-
19. Slovakia	2005	2008
20. Spain	2001	2010

21. Turkey	2010	-
22. United Kingdom	2001	2011
23. United States	2001	2006

Source: Council of Europe, 2014

Appendix I - Cyber legislation per country

Country	Type of legislation
5. Australia	• Cybercrime Act 2001 • Australian Security Intelligence Organization Act 1979 • Criminal Code Act 1995 • Telecommunications (Interception) Act 1997 • Australian Crime Commission Act 2002 • Credit Card Skimming Offences 2004 • Australian Anti-Terrorism Act 2005 • Australian Government e-Authentication Framework, 2005 • Australian Government Smartcard Framework 2006 • Australian Government Protective Security Manual, Attorney-General's Department 2005 • Australian Government Information and Communications Technology Security Manual 2006
6. Austria	• Criminal Law Amendment Act 2002 o (Strafrechtsanderungsgesetz 2002, 1166 d.B.)
7. Belgium	• Criminal Code 2002 – computer hacking o IV. Computer Hacking Article 550(b) of the Criminal Code
8. Canada	• Criminal Code 2003 amendment • Canada Evidence Act • Canada Criminal Code • Personal Information Protection and Electronic Documents Act • Federal prosecution under the Copyright Act • 1998 Criminal Code of Canada - Making, having or dealing in instruments for forging or falsifying credit cards -- s. 342.01(1)
24. Czech Republic	• Criminal Code 2005 amendment • Draft Act on Cyber Security

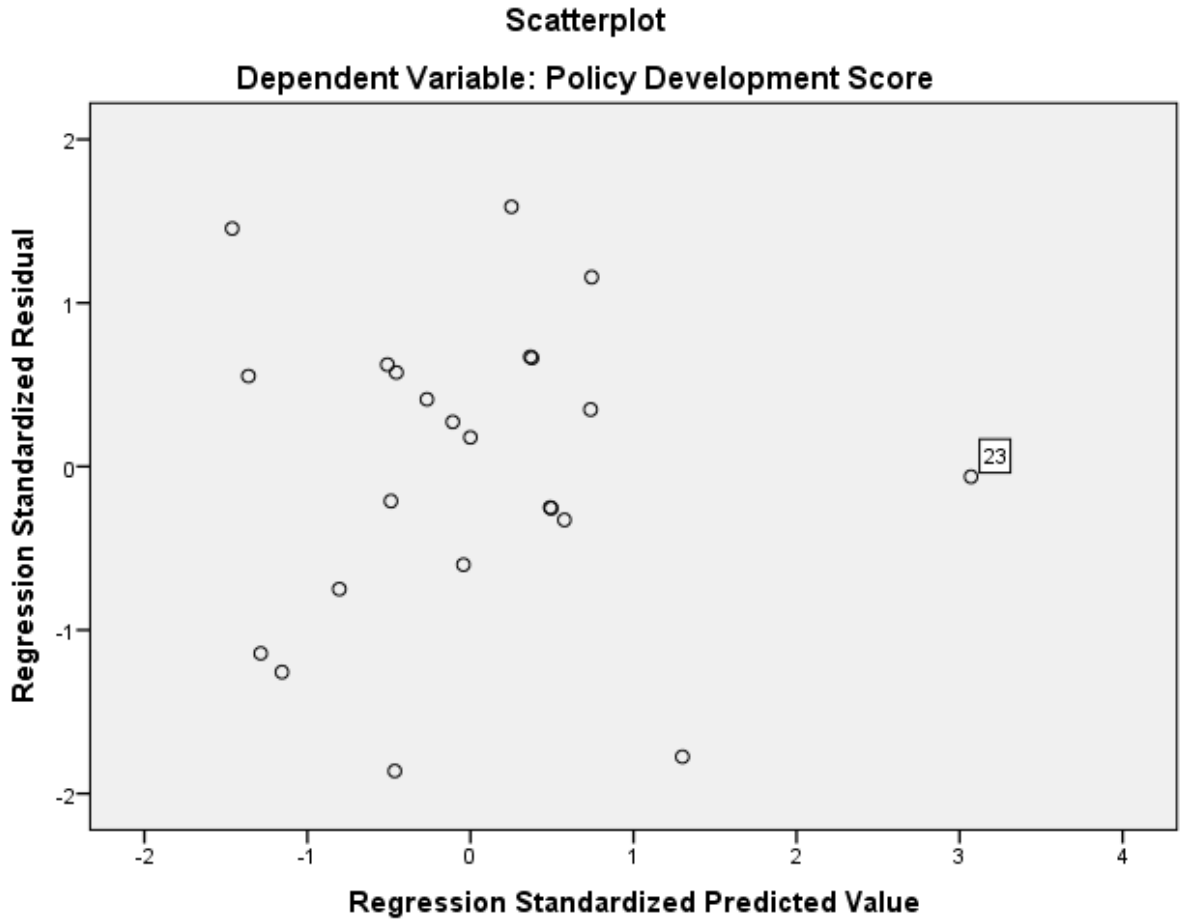
25. Denmark	• Penal Code 2003 o Penal Code Chapter 38 Section 8
26. Estonia	• Penal Code 2002 • Criminal Code Computer information crimes Article 268 • Computer Fraud; Article 269 • Deletion of computer information or software; Article 270 • Computer sabotage; Article 271. • Illegal use of computers, their systems or networks; Article 272. • Illegal interruption or blocking of the computer system connection; Article 273 • Obvious spread of computer viruses; Article 274 • Transfer of protecting codes
27. Finland	• Penal Code o Chapter 38 Section 8
28. France	• Amendment no.2004-575, Articles 323
29. Germany	• German Criminal Code • German Telecommunications Act • German Copyright Act
30. Hungary	• Penal Code amendment 2003 o Article 300 • 2013 Act on Electronic Information Security of Central and Local Government Agencies
31. Italy	• Penal Code amendment 2008 o Article 615
32. Latvia	• Criminal Law o Chapter XX, Articles 241-245
33. Lithuania	• Penal Code 2003
34. The Netherlands	• Criminal Code amendment 2006 o Article 138
35. New Zealand	• Crimes Act 1961 (Reprint at 1 June 2005) o Articles 249 - 254
36. Norway	• Penal Code Amendment 2003 o Section 145

37. Poland	• Penal Code o Part 3 Article 267 – 269
38. Slovakia	• Criminal Code 257a
39. Spain	• Penal Code amendment - Chapter I, Article 197, Section 1, Article 248 / 264 / 256 / 270, Section 2, Article 273
40. Turkey	• Criminal Code 1991 o Article 243 - 246
41. United Kingdom	• Police and Justice Act 2006 • Computer Misuse Act 1990 • Police and Justice Act 2006 Chapter 48 • The Computer Misuse Act of 1990 • The Regulation of Investigatory Powers Act 2000 • The Anti-Terrorism, Crime, and Security Act 2001 • Data Protection Act of 1998 • The Fraud Act 2006 • The Forgery and Counterfeiting Act 1981 • Privacy and Electronic Communications Regulations 2003 (EC Regulations)

42. United States	• United States Code • Homeland Security Act of 2002 (Amendments) • USA Patriot Act • Field Guidance on New Authorities that Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001 / 18 U.S.C. § 1029. • Fraud and Related Activity in Connection with Access Devices / 18 U.S.C. § 1030. • Fraud and Related Activity in Connection with Computers / 18 U.S.C. § 1362 Communication Lines, Stations, or Systems / 18 U.S.C. § 2510 et seq. • Wire and Electronic Communications Interception and Interception of Oral Communications / 18 U.S.C. § 2701 et seq. • Stored Wire and Electronic Communications and Transactional Records Access / 18 U.S.C. § 3121 et seq. • Recording of Dialing, Routing, Addressing, and Signaling Information • U.S.A. Sentencing Guidelines that Relate to Computer Intrusions • U.S.A. Sentencing Commission's Proposed Amendments to the Guidelines that Relate to Computer Intrusions

Source: CybercrimeData AS, 2014; Menting, 2011

Appendix J – Residuals



Residuals Statistics[a]

	Minimum	Maximum	Mean	Std. Deviation	N
Predicted Value	4,2147	9,0763	5,7826	1,07288	23
Std. Predicted Value	-1,461	3,070	,000	1,000	23
Standard Error of Predicted Value	,297	,969	,486	,162	23
Adjusted Predicted Value	3,9123	9,2031	5,8280	1,08802	23
Residual	-2,28420	1,94806	,00000	1,13997	23
Std. Residual	-1,862	1,588	,000	,929	23
Stud. Residual	-1,993	1,637	-,016	1,007	23
Deleted Residual	-2,61640	2,08766	-,04538	1,34602	23
Stud. Deleted Residual	-2,181	1,719	-,027	1,050	23
Mahal. Distance	,334	12,775	2,870	2,926	23
Cook's Distance	,001	,225	,046	,060	23
Centered Leverage Value	,015	,581	,130	,133	23

a. Dependent Variable: Policy Development Score

Appendix K – Diagnostics

Casewise Diagnostics[a]

Case Number	Std. Residual	Policy Development Score	Predicted Value	Residual
1	,348	7,00	6,5729	,42709
2	,272	6,00	5,6658	,33417
3	-,211	5,00	5,2594	-,25939
4	,663	7,00	6,1866	,81344
5	,623	6,00	5,2362	,76377
6	-,251	6,00	6,3074	-,30738
7	1,588	8,00	6,0519	1,94806
8	-,327	6,00	6,4011	-,40108
9	-1,775	5,00	7,1771	-2,17708
10	,671	7,00	6,1773	,82270
11	1,455	6,00	4,2147	1,78529
12	,178	6,00	5,7818	,21815
13	,553	5,00	4,3216	,67836
14	-1,143	3,00	4,4021	-1,40209
15	,411	6,00	5,4964	,50360
16	-1,862	3,00	5,2842	-2,28420
17	-,256	6,00	6,3140	-,31400
18	,575	6,00	5,2950	,70505
19	-1,257	3,00	4,5421	-1,54210
20	-,600	5,00	5,7364	-,73636
21	-,750	4,00	4,9197	-,91968
22	1,158	8,00	6,5800	1,42005
23	-,062	9,00	9,0763	-,07634

a. Dependent Variable: Policy Development Score

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	5,306	3,158		1,680	,109		
	Level of technological development	-,711	,397	-,418	-1,790	,089	,513	1,949
	Internet penetration	,003	,030	,025	,109	,915	,517	1,933
	Military expenditure	1,003	,360	,483	2,790	,012	,933	1,072

a. Dependent Variable: Policy Development Score

Collinearity Diagnostics[a]

				Variance Proportions			
		Eigenvalue	Condition Index	(Constant)	Level of technological development	Internet penetration	Military expenditure
1	1	3,662	1,000	,00	,01	,00	,01
	2	,215	4,131	,00	,27	,00	,30
	3	,119	5,536	,01	,11	,03	,57
	4	,004	29,980	,99	,61	,96	,12

a. Dependent Variable: Policy Development Score

Appendix L – Case summaries

Case Summaries[a]

	Mahalanobis Distance	Cook's Distance	Centered Leverage Value
1	1,13124	,00351	,05142
2	2,95114	,00487	,13414
3	,46684	,00083	,02122
4	1,09196	,01245	,04963
5	,56138	,00771	,02552
6	1,43882	,00215	,06540
7	,33434	,04175	,01520
8	1,14528	,00312	,05206
9	1,74758	,12582	,07944
10	1,25010	,01393	,05682
11	2,22988	,10488	,10136
12	5,15169	,00421	,23417
13	2,16863	,01476	,09857
14	1,90177	,05605	,08644
15	2,97263	,01115	,13512
16	1,83671	,14440	,08349
17	1,80590	,00269	,08209
18	2,02136	,01495	,09188
19	3,06088	,10799	,13913
20	5,55576	,05381	,25253
21	9,21640	,22484	,41893
22	3,18490	,09571	,14477
23	12,77482	,00428	,58067
Total N	23	23	23

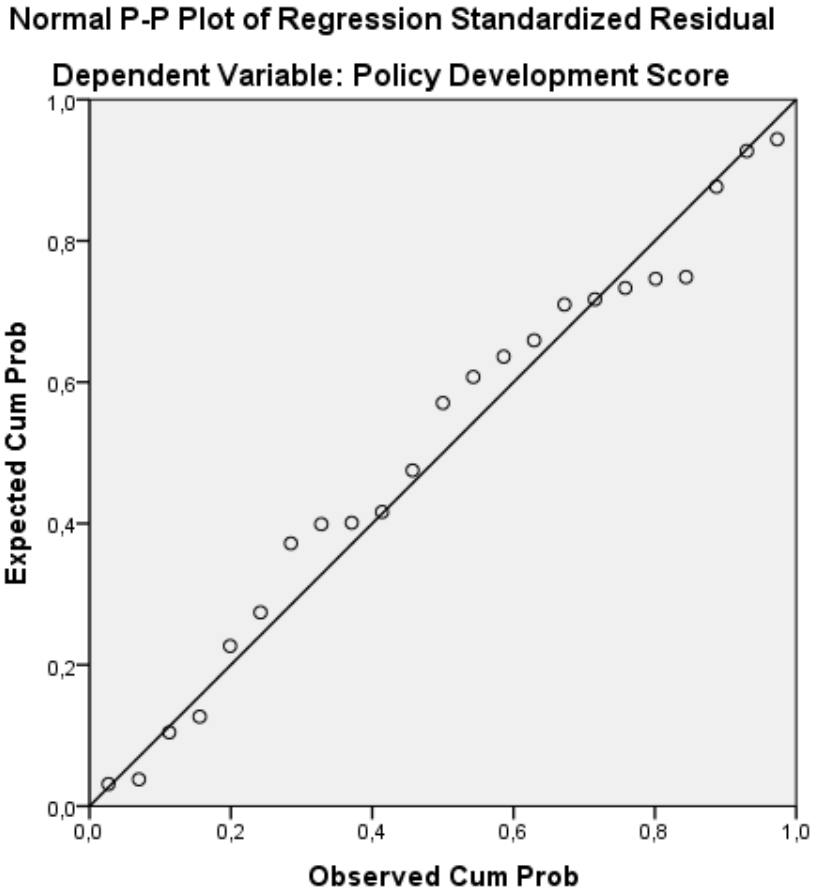
a. Limited to first 100 cases.

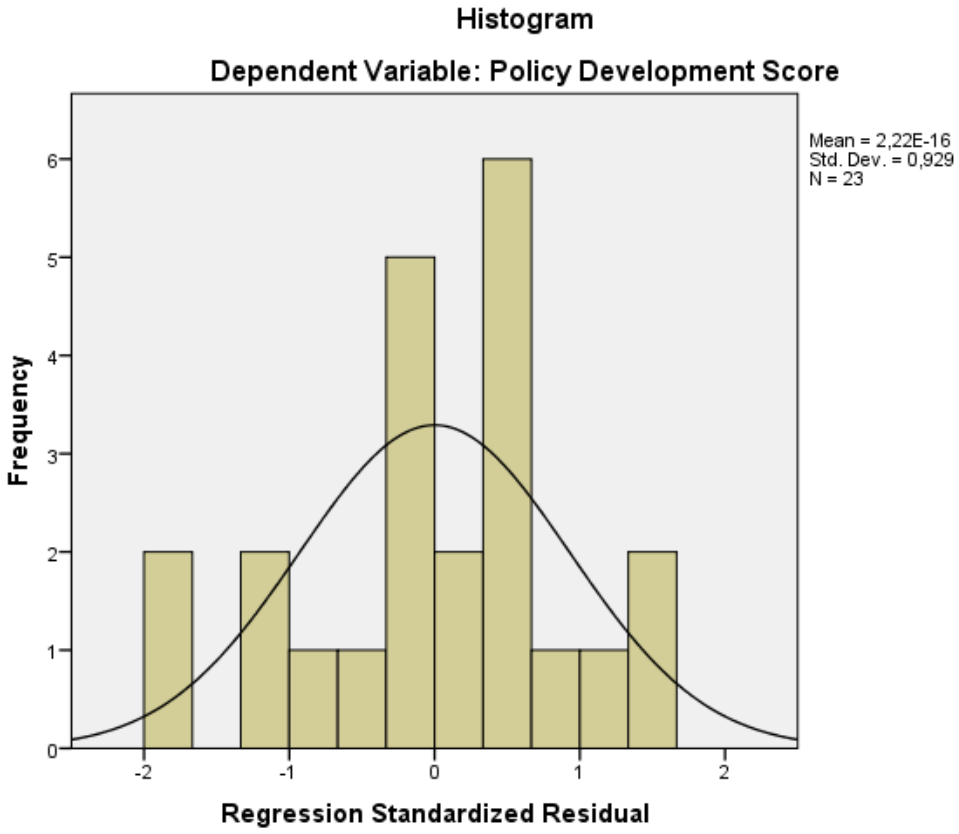
Case Summaries[a]

	DFBETA Intercept	DFBETA Technology	DFBETA Internet	DFBETA Military	Standardized DFBETA Intercept	COVRATIO
1	,17601	-,03252	-,00119	-,00043	,05444	1,33333
2	,29649	-,03945	-,00196	-,03267	,09159	1,48109
3	,02615	-,00559	-,00051	,00823	,00807	1,31400
4	,19657	-,04775	-,00038	-,02491	,06137	1,23442
5	,27590	-,01535	-,00202	-,03391	,08598	1,22033
6	,06657	,00569	-,00123	,00305	,02055	1,37257
7	-,32217	,04581	,00276	,07050	-,10713	,71801
8	,04465	,01120	-,00111	,00159	,01381	1,33873
9	-,36116	,12673	,00271	-,12861	-,12360	,61225
10	,35790	-,06290	-,00196	-,02966	,11178	1,24023
11	-,11925	,13020	,00156	-,10194	-,03941	,83028
12	,36169	-,02994	-,00360	-,00547	,11160	1,70281
13	-,16675	,05993	,00170	-,02918	-,05188	1,34141
14	-,20540	-,07221	,00222	,06174	-,06596	1,02648
15	-,51038	,05267	,00548	,00358	-,15815	1,44712
16	1,45386	-,16172	-,01689	,04493	,50381	,55655
17	,11348	,00193	-,00172	,00198	,03504	1,39744
18	,02882	,04004	-,00140	,02774	,00897	1,32373
19	1,21022	-,21465	-,01164	,01834	,39354	,98868
20	-1,31016	,15139	,01066	,09080	-,40933	1,58094
21	-,79779	-,09005	,01324	-,10009	-,25293	1,84136
22	-1,40213	,13680	,01240	,15807	-,45222	1,06314
23	,06409	,00364	-,00017	-,04300	,01976	3,29586
Total N	23	23	23	23	23	23

a. Limited to first 100 cases.

Appendix M – Standardized residuals graphs





Appendix N – Scale reliability

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
,706	,706	3

Item Statistics

	Mean	Std. Deviation	N
Legal Foundation	1,9565	,70571	23
Agency Responsibility	1,8696	,62554	23
International Cooperation	1,9565	,63806	23

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
Legal Foundation	3,8261	1,150	,530	,510	,612
Agency Responsibility	3,9130	1,538	,336	,221	,823
International Cooperation	3,8261	1,059	,749	,590	,321

Appendix O – SPSS output (excluding TD)

Regression analysis - model summary (excluding TD)

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.617[a]	.380	.318	1.29253

a. Predictors: (Constant), Military expenditure, Internet penetration

Regression analysis - ANOVA (excluding TD)

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	20.500	2	10.250	6.136	.008[b]
	Residual	33.413	20	1.671		
	Total	53.913	22			

a. Dependent Variable: Policy Development Score

b. Predictors: (Constant), Military expenditure, Internet penetration

Regression analysis - coefficients (excluding TD)

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.758	1.977		.383	.706
	Internet penetration	.041	.023	.313	1.772	.092
	Military expenditure	1.161	.367	.559	3.161	.005

a. Dependent Variable: Policy Development Score

Appendix P – SPSS output

Multiple regression analysis - model summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.685[a]	.470	.386	1.22667

a. Predictors: (Constant), Level of technological development, Military expenditure, Internet penetration

Multiple regression analysis - ANOVA

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	25.324	3	8.441	5.610	.006[b]
	Residual	28.589	19	1.505		
	Total	53.913	22			

a. Dependent Variable: Policy Development Score

b. Predictors: (Constant), Level of technological development, Military expenditure, Internet penetration

Multiple regression analysis – coefficients

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	5.306	3.158		1.680	.109
	Internet penetration	.003	.030	.025	.109	.915
	Military expenditure	1.003	.360	.483	2.790	.012
	Level of technological development	-.711	.397	-.418	-1.790	.089

a. Dependent Variable: Policy Development Score