European Cyber Security: a Cyber Deterrence Approach

juni 11

2013

With the establishment of the EC3 (European Cyber Crime Centre), a new framework has been introduced by the Commission to enhance Europe's cyber security. Where the old framework has failed to prevent the second largest attack in the world (the 2007 attacks on Estonia) and to reduce the ever growing numbers of cybercrimes, the new framework is expected to improve Europe's cyber security significantly. Using Goodman's conceptualisation of cyber deterrence, the extent to which this new framework is able to deter cyber-threats is analysed.

Prologue

Although, the conclusions and findings of a report seemingly show the insights and knowledge gained by a student over the period of approximately 3 months, the knowledge and lessons that I have obtained are quite frankly from another source. During this period I have gained experience in discipline, determination and the crucial understanding that a ‘paragraph’ is something very different to a ‘section’. I have had the pleasure of gaining knowledge in what appears to be the future of this world in terms of communication, warfare, entertainment and information. I have had the experience of physically having to stand up and walk around because it felt like bits of the enormous pile of information inside my head could fall out and I wanted to pick it back up. As a result of all these timeless experiences a thesis, of which I am very proud, has been finalised. A thesis that has required my supervisor to answer many superfluous mails, sit many sessions and read many, many below par texts. Therefore, I would like to thank Dr. M.R.R Ossewaarde for his time, dedication and devotion in this cause; as a source of inspiration with his sharp-minded remarks, as a source of information with his mails ‘for your eyes only’ and as a colleague, rather than supervisor, in our small cyber security council.

Table of Content

1. Introduction

May 10th 2007, the Estonian CERT (Cyber Emergency Response Team), with the help of the international community, was able to prevent the second largest cyber-attack in the history of the world from shutting down Estonian critical infrastructures (Shackelford, 2009). Although Europe was able to defend a MS (Member State) from total collapse, a significant amount of damage was dealt. January 24th 2008, Estonian police and legal system successfully found and convicted a Russian student for posting a fake letter of apology on the Estonian prime minister's website for removing a symbolic Soviet statue. He was fined $ 1.642,- and was the only person to be convicted after the tens of thousands of attacks during the three week siege. The conclusion; Europe proved unable to prevent, or punish (sufficiently), a cyber-attack on European infrastructures.

January 1st 2013, the EC3 (European Cyber Crime Centre) is officially established as an institution within Europol. The EC3 is only one of the measures inherent to the new Commission strategy for "an open, safe and secure cyberspace" (Commission, 2013). These measures are to, amongst others, strengthen the Union's capacity and ability to fight cybercrime. Moreover, they are the reaction on the growing inequality in the distribution of power between the incapable governments and very capable 'abusive' perpetrators (Prins, 2012). To this end, the European cyber security framework has developed as a response to the threats it is facing in the cyber realm. This responsive way of working leads to being one step behind aggressors who find increasingly cunning ways of incurring costs on European citizens and infrastructures (Cullifo et all, 2012). However, the EU faces more than just cybercrimes; scholars have argued and warned for various other sources of cyber-threats such as "cyber warfare" (Carr, 2012), "cyber terrorism" (Wilson, 2008) and "state-sponsored cyber-attacks" (Shackelford, 2009). To this end, Europe needs a strong and preventive cyber security strategy/framework to ensure fundamental freedoms of its citizens as well as protect key areas of interest (Commission, 2013). This thesis seeks to analyse the extent to which the European cyber security framework is able to deter cybercrimes and state-sponsored cyber-attacks in the light of Goodman's "cyber deterrence" theory (2010). By assessing the strengths of the European cyber security framework in the light of the cyber deterrence theory, policy proposals can be made to strengthen the ability to prevent rather than cure the damages dealt to key European interests.

Deterrence theories in general are based on the idea that people consciously avoid pain. By making a choice painful enough; people will be refrained from making that choice (Nagin, 2011). Formulated differently deterrence theory proposes important attributes which, if maximized, provide for an effective tool to refrain aggressors from attacking, regardless of their motives. Cyber deterrence is the deterrence theory being superimposed to the cyber domain. Cyber deterrence rather than deterrence theory is relevant to assess the strength of the European cyber security framework, because cyber-threats are different to traditional threats; they lend themselves to anonymity. To this end, cyber deterrence theory emphasizes other factors, such as ‘attribution’ (Zimmerman, 2013; Goodman, 2010; Guitton; 2012). The strengths of using cyber deterrence is threefold, first of all, the future is potentially filled with cyber wars. Secondly, history has shown the efficacy of deterrence in other domains, e.g. the nuclear deterrence during the cold war. Finally, the relative low costs of using a (cyber) deterrence strategy rather than incurring cyber related costs (Goodman, 2010). All in all then, cyber deterrence is an effective and efficient theory that currently is used to either apply as a security strategy in the US (Shackelford, 2009; Zimmerman, 2013), or to analyse incidents where it has failed; such as Estonia and Georgia (Goodman, 2010). Conversely, this thesis seeks to apply the available knowledge on cyber deterrence to the newly formulated cyber security strategy; predicting Europe’s future capabilities.

The main interest of this thesis can be translated into the following research question: *to what extent is the European cyber security framework able to deter cyber-threats?* The concept of cyber-threats is used to include different types of threats; this thesis is interested in cybercrimes and state-sponsored cyber-attacks. The former is the most common source of threats, whilst the latter is thought to, potentially, be the most destructive type of threat. The extent to which Europe is able to deter an enemy is assessed using Goodman’s cyber deterrence theory. To this end, the ability to deter depends on the extent to which the European cyber security framework reflects the necessary elements as highlighted by Goodman. Goodman’s framework in particular is chosen due to its comprehensiveness and its prior application to assess Europe’s deterrence capabilities for the out—dated, pre-2013, cyber security strategy. The new framework will be re-assessed by this thesis.

In order to answer the research question, three steps will be taken; first of all, the concept of cyber deterrence will be defined, conceptualised and operationalized in order to establish the elements necessary to enable deterrence. At the core of this step are the writings of Goodman (2010), Geers (2010) and Cullifo et all (2012). Secondly, the European cyber security framework will be scrutinised in terms of the elements highlighted by cyber deterrence. At the core of this step are the Commission strategies to establish and enhance Europe’s cyber security, as formulated in the Commission communication of (2009) and (2013). These communications highlight the specific measures taken to enhance Europe’s cyber security. Thirdly, the extent to which the cyber security measures reflect the cyber deterrence elements will be assessed. Using the conceptualisation of the key cyber deterrence authors; the separate elements will be combined to conclude whether or not the European cyber security framework will be able to deter cybercrimes or state-sponsored cyber-attacks.

2. Conceptualizing Cyber Deterrence

The ability to deter an adversary in the cyber domain depends on the execution of various elements of the cyber deterrence theory. This chapter seeks to shed light upon the elements, or variables if you will, to acquire/maximize the ability to deter (potential) adversaries. The key function of this chapter is to specify the cyber deterrence variables on the basis of which the European cyber security framework will be assessed. To this end, this section will define the key concepts: cybercrime, state-sponsored cyber-attacks and cyber deterrence. The definition of cybercrime and state-sponsored cyber-attack are relevant because this thesis seeks to assess Europe's ability to deter these two cyber-threats. Secondly, the ability to deter will be conceptualised using cyber deterrence theory. This will be done by using, primarily, Goodman (2010), Geers (2010) and Cullifo et all (2012). Finally, the dialectic amongst cyber deterrence authors, and critique aimed at cyber deterrence, will be highlighted and taken into account for the methodology, analysis and concluding section.

The first of the three crucial definitions is cybercrime. Although there are various definitions of cybercrime[1], the working definition that is going to be central throughout the report is that of the Commission. The main reason for this is that the Commission basis its cyber deterrence framework on its own conceptualisation, using a different conceptualisation may skew the reliability of the data and Europe's ability to deter cybercrime. The Commission defines cybercrimes as: "crimes related to the computer and internet" (2013). The Commission distinguishes between internet and computer specific crimes 'new crimes' and the use of internet and computers to commit 'traditional crimes' e.g. incitements to violence on the internet (Commission, 2013). The specific type of cybercrimes, which are penalised, and their sub-types are formulated in the Council Convention on Cybercrime[2]; of which almost all EU MSs are signatories.

The second definition; state-sponsored cyber-attack, seems straight forward, yet isn't. The name suggests the use of a 'cyber-attack': "efforts to alter, disrupt, or destroy computer systems or networks or the information or programs on them" (Waxman, 2011), by a nation state. However, it is very difficult to identify which cyber-attack was a state-sponsored attack; Clapper argues that radical 'hacktivist' groups could also disrupt financial networks and bring forth other (unintended) consequences which might be misinterpreted as a state-sponsored attack (2013). To this end, Richard Clarke and Robert Knake's definition of 'cyber warfare': "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption" (2010), provides for a simple and clear idea of what a state-sponsored cyber-attack would look like. This definition has been used by George W. Bush and is currently still used in the US senate.

The third and final definition, which is used throughout the report, is; 'cyber deterrence'. But what is cyber deterrence[3]? Various definitions of cyber deterrence exist; Gibb's and Guitton argue that deterrence occurs when an offender refrains from a criminal activity because he/she fears the punishment (Gibbs, 1985; Guitton, 2012). Similarly Cullifo et all state that deterrence seeks to cause an adversary to refrain from acting by influencing its belief that the likelihood of success is slight, or that the pain from the response is greater than it is willing to bare (2012). Contrary to the previous authors, Geers argues that deterrence is a military strategy with the purpose of preventing rather than winning wars (2010). All in all, although these cyber deterrence theories differ in their definition of what cyber deterrence really entails, they do share the basic idea behind deterrence itself; that people consciously avoid pain (Nagin, 2011). However, in order to answer the research question not only the definition, but moreover the conceptualisation of cyber deterrence is required.

Acquiring the ability to deter requires maximizing certain cyber deterrence elements. However, different scholars argue for different conceptualisations of cyber deterrence and thus a different set of variables that require maximization. Goodman presents eight factors which, in his work; "Cyber Deterrence; Tougher in Theory than in Practice?" are fundamental to cyber deterrence theories (2010). The first variable that Goodman highlights, similarly to Goodpaster et all (1997), is '*interest'*: a deterrence strategy is applied when a state seeks to protect an interest. Although very few authors actually make this factor explicit, the protection of an interest is an (implicit) incentive for applying a (cyber) deterrence theory in the first place. The specific interest that the actor seeks to protect can be anything worthwhile to protect. The second variable is the '*deterrence declaration'*: this declaration is made explicit verbally or on paper in order to deter adversaries from engaging in any activity that compromises the interest that the state seeks to protect, similarly (Wheatly and Hayes, 1996). A deterrence declaration is expected to state the (retaliatory) measures that an actor will take if aggressed upon; 'if you do X I will do Y'. To this end, Goodman highlights two means to ensure the deterrence declaration; '*denial measures'* and '*penalty measures'* (2010). Lan et all combine both denial and penalty measures under a variable called 'response': the ability to respond to an attack (2010). For Goodman, however, the denial measures are the defensive capabilities of the actor, and are sub-divides in terms of two attributes; 'prevention': preventing the aggressor from mounting a successful attack, and 'futility': rendering a successful attack futile by preventing the desired outcome, similarly (Long, 2008; Kugler, 2009). Goodman's 'penalty measure' entails the prevention of the adversary's aggression by threatening greater aggression and consists of three attributes; 'retaliation': attacking the aggressor to impose costs that outweigh the attackers benefits, 'interdependency': the commonality of an interest may increase the cost and/or reduce the benefits gained by the aggressor, similarly (Feaver, 1998), and 'counter productivity': retaliation against a strategic asset of the aggressor e.g. family to counter the aggressors success on a tactical goal e.g. shutting down critical infrastructures. Both denial and penalty measures can be used to deter an adversary. However, the strength of the deterrence declaration lies not only with the ability to execute it, moreover it is dependent on the extent to which the potential aggressor perceives this declaration as credible and reassuring.

'*Credibility'* for Goodman is the extent to which potential aggressors belief that the defender has the capability and will to apply the measures as stated in the deterrence declaration (2010), similarly (Wheatley and Hayes, 1996; Geers, 2010; Cullifo et all, 2012). Moreover, the '*reassurance'* measure relates to the level of certainty potential aggressors have that if they commit a cybercrime or cyber-attack, the countermeasures and penalties, as described in the deterrence declaration, will be executed (2010). Kugler adds that the reassurance measure should also be used for non-aggressors; if they do not attack, they should be reassured that no harm will come to them (2009). Goodman's reassurance measure is to some extent dependent on Guitton's 'attribution'; the ability to find a perpetrator (2012), or according to Lan et all; understanding who has attacked you (2010). To this end, the ability to reassure, rather than the speed of, attribution is important for cyber deterrence (Goodman, 2010).

Additionally, Goodman highlights two final variables; '*fear'* and '*cost-benefit calculation*'. 'Fear' plays in important role towards deterring potential aggressors; the more afraid an actor is for the denial and penalty measures, the less likely he/she is to aggress (Goodman, 2010; Long, 2008). Although fear is not explicitly mentioned by other authors, it is implied by all (cyber) deterrence theories. Being unable to put fear into an aggressors heart will result in the inability to deter this person. Conversely to Goodman, Guitton applies the concept of fear in an entirely different manner. Although Guitton implies that fear is required in order to deter an aggressor, the actual concept of fear is used by him to highlight the inability of governments to reassure the attribution of perpetrators because companies fail to report incidents. Guitton Argues that fear for negative media attention is the reason that, to a large extent, companies fail to report cyber-attacks on their companies (2012). The final variable that Goodman highlights as valuable for cyber deterrence theory is 'cost-benefit calculation'; every aspect of cyber deterrence must be cost-benefit friendly (Goodman, 2010). Having a cyber deterrence strategy altogether depends on whether or not it is cost-benefit friendly (Goodman, 2010; Long, 2008; Pratt et all, 2006). Although very few authors highlight this aspect, some argue that applying a cyber deterrence strategy is worthwhile since the costs of the collapse of critical infrastructures are far larger than the implementation of the necessary cyber deterrence variables (Kshetri, 2010; Goodman, 2010; Cullifo et all, 2012).

The second cyber deterrence author, whose conceptualisation will be highlighted, is Geers. In specific, light will be shed upon his work “The Challenge of Cyber-Attack Deterrence” (2010). Similarly to Goodman, Geers highlights ‘*deterrence declaration’* as an important variable in cyber deterrence theory. However, Geers adds that the deterrence declaration must be written clearly and “leave no doubt” as to the ability and willingness to perform the declaration (2010). Also, Similarly to Goodman, Geers highlights ‘*denial’* and ‘*penalty’* as relevant variables. However, conversely to Goodman, Geers identifies the two variables as two distinct cyber deterrence strategies (2010). As a result, ‘denial measures’ entails the prevention of the adversary from acquiring threatening technology, and is subdivided in three relevant aspects: ‘*capabilities’* ‘*communication’* and ‘*credibility’* (2010). ‘Capabilities’ refers to the ability, in terms of resources and tools to apply the denial measure. ‘Communication’ refers to internal and international cooperation for establishing common norms and legal measures against cyber-threats. The final aspect of the denial measures, according to Geers is ‘credibility’. This measure highlights the importance, not so much of the actual ability of doing something, but being able to do so in the eyes of the adversary. This indicator generally scores low (Geers, 2010). ‘*Penalty measures’*, means the prevention of aggression of the adversary by threatening greater aggression (Geers, 2010). Similarly to the denial measures Geers establishes three indicators: ‘*capabilities’* ‘*communication’* and ‘*credibility’*. All three indicators are similarly used and defined as those for ‘denial measures’. However, Geers adds that the ‘credibility’, in practice, for denial measures is lower than that of penalty measures. Moreover, in addition to his general cyber deterrence theory, Geers adds that the concept of ‘attribution’ and ‘asymmetry’ are important to mention. Attribution refers to the ability of the defending state to locate the aggressor, similarly (Goodman, 2010; Guitton, 2012; Lan et all, 2010; Cullifo et all, 2012). Asymmetry refers to the uneven distribution of power in the cyber domain (Geers, 2010), conversely, Goodman argues that in terms of power, individuals become states in cyberspace (2010).

The third, and final, authors are Cullifo et all. In their article “A blueprint for cyber deterrence: building stability through strength”, Cullifo et all conceptualise cyber deterrence using three measures; ‘signaling’, ‘attribution’ and ‘credibility’ (2012). Similarly to Goodman and Geers, Cullifo et all argue that ‘signalling’ should convince potential adversaries that the costs of the retaliation will outweigh their perceived benefits (2012). In addition to these three authors, Guitton argues that a singular ‘deterrence declaration’ Goodman (2010), ‘signalling’ Cullifo et all (2012) or ‘transparency’ Lan et all (2010), is not enough. In order to effectively deter potential aggressors the deterrent messages need to be constantly updated and re-expressed (2012). The second variable Cullifo et all highlight is ‘attribution’. Similarly to Geers and Goodman, Cullifo et all conceptualise it as the ability to trace a perpetrator, and argue that it is a crucial, yet hard to pull off, element. Thirdly, similar to

Goodman and Guitton, Cullifo et all highlight the importance of 'credibility'. 'Credibility' for Cullifo et all entails the capability and political willingness to apply the full range of cyber-capabilities to counter-attack, as well as defend against the adversary (Cullifo et all, 2012). Moreover, to become credible in the eyes of the potential aggressor, Cullifo et all argue that 'showing off' your cyber-capabilities is necessary (2012), similarly (Lan et all, 2010). However the analogy between nuclear deterrence and cyber deterrence might be the reason for making the 'mistake' of 'showing off' your cyber-capabilities. In the era of nuclear deterrence, showing off you capabilities gave the adversary the certainty of destruction in case of aggressing, without allowing it to copy and use the means. In cyberspace, however, showing off your weapons will allow the adversary to easily trace and use these weapons against you or develop technology to bypass your threat (Cullifo et all, 2012). Cullifo et al propose to solve this problem by demonstrating offensive capabilities, yet leaving critical elements out, to avoid the adversary from gaining the knowledge (2012).

To compare the three distinct conceptualisations; Goodman's conceptualisation is closely related to that of Cullifo et all. However, Goodman's framework provides for more, in depth, variables and to measure cyber deterrence. Similarly to Goodman, Geers' conceptualisation is very comprehensive, however it highlights different variables and indicators. For example, where Goodman defines denial measures as the ability to fend off an attack, Geers seeks to prevent a potential attack. As a result, Geers' approach seems (more) fit to cyber deterrence, however it is a rather utopic approach compared to Goodman's practical approach. Geers' denial strategy is highly impractical because it is very difficult to see what the adversary is actually doing at the moment let alone denying him access to the internet (Lan et all, 2010; Zimmerman, 2013; Goodman, 2010). Therefore, preventing a threatening technology to fall in the hands of the adversary is close to impossible in the cyber realm. Secondly, Geers' utopic conceptualisation is most likely to be built upon the nuclear deterrence analogy. Conversely, in the cyber-realm the most likely scenario is that potential aggressors already have the threatening technology and governments respond to, rather than prevent, these threatening technologies (Cullifo et all, 2012).

Despite the disparities concerning the conceptualisation of cyber deterrence, the general critique aimed at cyber deterrence has been left unattended. Many scholars, but also NGO's and politicians, have criticized deterrence for producing and maintaining the threat of MAD (Mutually Assured Destruction) during the cold war era. They have argued that disarmament should take place from both sides (Beth, 2008). The search of cyber deterrence scholars to establish MAD (Mutually Assured Disruption) threatens to throw cyber deterrence (back) under the same train (Pendall, 2004; Derene, 2009; Geers, 2010). Moreover, cyber deterrence is criticized for its assumption of rational behaviour based on perfect knowledge. Jacob (1978) argued that decisions are not always made rationally.

Similarly, Guitton argued that cybercrimes are cause by impulse rather than ration choice (2012). Goodman himself argues that perfect information is never available and that emotions, interests and politics play a role in decision making (Goodman, 2010; Guitton, 2012).

This chapter has provided for the definitions of the main concepts; cyber deterrence, cybercrime and state-sponsored cyber-attacks. These definitions have helped to establish an understanding of what the cyber-threats are that Europe seeks to defend itself against, and moreover, what it means to deter these cyber-threats. To this end, cybercrime is any crime aimed at, or using means like, computers, internet and cyber-infrastructures. State-sponsored cyber-attacks are, similarly, based on old principles that have been expended to the cyber domain. Finally, cyber deterrence is the, during the cold war, proven concept of deterrence that has been superimposed to the cyber domain. The conceptualisation of cyber deterrence has provided the theoretical construct that enables the assessment of the European cyber security framework's ability to deter cybercrimes and state-sponsored cyber-attacks. To this end, Cullifo et all have provided a clear-cut, yet shallow, conceptualisation of the key variables. Geer's conceptualisation, on the other hand, has proven to be more elaborate. However, although cyber deterrence is a theory, Geer's variables were rather utopic and impossible to assess. Finally, Goodman's conceptualisation of cyber deterrence has proven to be both practical and elaborate. It has already been applied to cases such as Estonia (Goodman, 2010) and Goodman has researched and combined all (necessary) elements of cyber deterrence in order to formulate his conceptualisation (2010). Goodman's eight variables can be used to operationalize cyber deterrence and subsequently analyse the extent to which the European cyber security framework reflects these variables. As a result, the extent to which the European cyber security framework is able to deter cyber-threats can be assessed. To this end, the next chapter contains the operationalization of the key concepts, method of data collection and method of analysis.

3. Operationalizing cyber deterrence

Europe's ability to deter will be determined through the compatibility of the cyber security framework's measures to the cyber deterrence variables. To this end, first of all, the cyber security framework needs to be scrutinised in order to establish the relevant measures that Europe has already, or has proposed to, set in place. Secondly, the concept of cyber deterrence must be operationalized in order to assess the strength of Europe's cyber security measures, in terms of cyber deterrence. This chapter, then, seeks to construct the guidelines for answering the research question by; first of all, highlighting the specific datasets from which Europe's cyber security measures can be scrutinised, and secondly, by operationalizing and establishing a measure for cyber deterrence using Goodman's conceptualisation.

3.1. Data collection

This sub-paragraph will highlight the specific data sets that are used to scrutinise the European cyber security framework. The main quandary that has been attended is whether to use the current, to date implemented, cyber security framework, or to use the proposed, future, cyber security framework under the 2013 cyber security strategy. Ultimately, the choice was made to scrutinise and analyse the (proposed) future cyber security framework. The current cyber security framework consists of two elements; the partially implemented 2009 cyber security strategy and the partially implemented 2013 cyber security strategy. As a result, there are various uncertainties related to the implementation of the 2013 cyber security framework, e.g. which protocols of which strategy is used currently? And, which protocols of the former strategy will be overruled, and when? These uncertainties make it difficult to formulate valid conclusions without the risk of being overtaken by events. Conversely, there is a high certainty for what these institutions are intended to do. To this end, applying cyber deterrence theory to the proposed cyber security framework, according to the 2013 Commission cyber security strategy, will highlight the strengths and weaknesses of Europe's ability to deter an adversary once fully established. As a result, the uncertainties related to the transition between the two strategies are avoided. However, as the following sections will point out, the 2013 cyber security strategy will not be the only point of reference in terms of strategies, there are numerous measures of the 2009 cyber security strategy that are left unchanged and are thus still used under the future cyber security framework.

After establishing the timeframe, three types of data are selected to be used for the scrutiny and assessment of the European cyber security framework; legal documents, policy documents and institutions' websites. First of all, legal documents are documents such as the UN (United Nations) charter; in specific article 2(4)[4]. This article withholds states from (cyber) retaliation if not in line with the UN principles. Moreover, it provides for international guidelines for defence and retaliatory measures and competencies, both amongst European MSs and between EU MSs and third-countries. Secondly, the TFEU (Treaty on the Functioning of the European Union) is an important dataset; in specific article 222, the solidarity clause[5]. This article enables MSs to act jointly, using any means, to prevent, protect and assist a MS under threat of a man-made (cyber) disaster or (cyber) terrorist attack. This article provides for the intra-European guidelines for retaliatory and defensive measures and competencies. Finally, the Council Convention on Cybercrime (2001)[6] is another key legal document. It provides for the criminalisation of specific cybercrimes and sub-groups thereof and is signed and ratified by almost all European countries as well as third-countries.

The second type of data, are policy documents. These documents provide for data on the competencies and capabilities of institutions and protocols of the European cyber security framework. However, the policy documents that are going to be used as datasets are somewhat different than directives or regulations. The Commission communications 'on critical information infrastructure protection' (2009A) and 'for an open, safe and secure cyberspace' (2013) are the key policy documents. The two documents entail the Unions cyber security strategies, subsequently; 'the CIIP (Critical Information Infrastructure Protection) action plan' and the current 'Strategic Priority System'. However, these documents are non-binding since "A non-binding approach will be more effective in steering a dialogue through which interested parties can work out the best way to cooperate and share best practices" (Commission, 2009B). As a result, the measures proposed in these communications are not necessarily implemented immediately/fully by MSs. This aspect portrays a potential, yet inevitable, bias in the outcomes of the research, which needs to be taken into account. Nevertheless, the Commission communications form a core insight of how the finalised cyber security framework will function and how the institutional competencies will be distributed. Applying cyber deterrence theory to this framework will highlight the strengths and weaknesses of Europe's ability to deter an adversary once fully established.

The final type of data that will be used for scrutinising the European cyber security framework, on the basis of cyber deterrence elements, are the websites of key institutions such as: the EC3[7] (European Cyber Crime Centre), which is established within EUROPOL and has a mandate to aid in the investigation and prevention of cybercrimes. EUROPOL[8] is the European law enforcement agency, its mandate is far beyond cyber related issues e.g. drug, human trafficking and fraud. Another key institutions is ENISA[9] (European Network and Information Security Agency), which has various competencies ranging from raising public awareness to developing a best practice guideline for MSs to establish national CERT's. Additionally, EUROJUST[10] seeks to support cross border investigations by, amongst others, enhancing the coordination and cooperation between the investigation and prosecution authorities bilaterally. Moreover, the ENCS[11] (European Network for Cyber Security) seeks to pool knowledge and resources, for the use of MSs, to help protect European CII's. Finally, the EGC[12] (European Government Cyber emergency response team) seeks to foster mutual cooperation and information sharing amongst its, growing amount of, members. All in all, these websites provide for important information related to the goals and competencies of these institutions within the European cyber security framework. Moreover, they provide for additional information regarding the institution itself such as; agenda, staff and the latest updates.

3.2. Data Analysis

This sub-paragraph seeks to establish the necessary, chronological, steps to answer the research question. This will be done by; first of all, highlighting the necessary variables using Goodman's cyber deterrence theory and secondly by arguing a level of measurement for these variables. Based on the compatibility of Europe's cyber security framework with these cyber deterrence variables, Europe's ability to deter cybercrime and state-sponsored cyber-attacks will be assessed.

The selection of the relevant European cyber security elements will be based on Goodman's conceptualisation of cyber deterrence. Goodman's conceptualisation of cyber deterrence is used for threefold reason; first of all, Goodman's conceptualisation has made cyber deterrence elements, that are implied or assumed by other scholars, explicit. To this end, he formulated cyber deterrence elements that are fundamental to all cyber deterrence theories (Goodman, 2010). Secondly, Goodman is one of the very few scholars to actually apply cyber deterrence in a European context; cyber deterrence is primarily a strategy envisioned by and for the US due to its nuclear deterrence history, e.g. Shackelford (2009). Finally Goodman's conceptualisation is more comprehensive and practical as compared to the conceptualisation of Cullifo et all (2012) and Geers (2010). To this end, on the basis of the variables Goodman conceptualised, data-sets will be scrutinised to find; declarations, institutions, legal measures, means of cooperation and other protocols that reflect Europe's ability to deter. Table 1 portrays these eight variables:

Table 1: Key variables and indicators reflecting cyber deterrence and the subsequent assessment thereof

Variable	Indicator	Measurement range
Interest	*	*Availability:* Very explicit – very implicit
Deterrence declaration	*	*Strength of formulation:* Very strong – very weak
Denial measures	Prevention	*Ability to prevent*: Very strong – very weak
	Futility	*Ability to render futile:* Very strong – very weak
Penalty measures	Retaliation	*Ability to retaliate:* Very strong – very weak
	Interdependency	*International relations:* Very strong – very weak
	Counter productivity	*Ability to target and retaliate:* Very strong – very weak
Credibility		*In the eyes of the aggressor:* Very credible – very unconvincing

Reassurance	*	*Ability to ensure declaration:* Very strong – very weak
Fear	*	*Ability to threaten:* Very strong – very weak
Cost-benefit calculation	*	*Ratio:* Very worth – not worth at all

* Note that these variables will be measured directly, without indicators, based on the conceptualisation by Goodman (2010).

The third column of the table represents the measurement of each variable and indicator. By using a scale type measure, the relative strengths and weaknesses of the European cyber security framework, in terms of the cyber deterrence theory, can be made explicit. The actual measure appointed to each variable is based on the normative assessment of each variable using, primarily Goodman's, cyber deterrence theory, but also Cullifo et all (2012), Lan et all (2010), Guitton (2012), Geers (2010) and O'Connel (2012). A normative scale measurement allows the research question to be answered more precisely in terms of 'the extent to which' the EU is able to deter potential cyber-threats. Moreover, since the relative weakness of each variable can be assessed, policies can be proposed in the conclusion paragraph to improve specific aspects of the European cyber security framework in order to be able, or improve the ability, to deter. It should be emphasized, however, that the ability to deter refers to the deterrence of cybercrimes and state-sponsored cyber-attacks. deterring cyber threats in general is not viable since every type of threat has to be tackled differently. To this end, it is important and interesting to analyse Europe's ability to deter the most common type of cyber threat; 'cybercrimes' and possibly the most destructive form of cyber-threats; 'state-sponsored cyber-attacks' as had happened in Estonia (2007).

This chapter has establish a guideline to answering the research question which entails, first of all, the use of legal documents, policy papers and institutional websites to scrutinise the European cyber security strategy/framework in terms of the variables, summarised in table 1, as conceptualised by Goodman. The compatibility of the European protocols, (legal) frameworks, institutions and their competencies to Goodman's cyber deterrence variables will be scrutinised and highlighted. Secondly, using scholarly writings such as Cullifo et all (2012), Geers (2010) and Goodman (2010), the compatible elements of the European cyber security framework will be compared to the theoretical ideal type constructed by these cyber deterrence scholars. Taking all variables together, the research question, in terms of the extent to which the European cyber security framework is able to deter, can be answered. Finally, the findings that do differ from how cyber deterrence authors have conceptualised it allow for policy proposals to be made in order to strengthen Europe's ability to deter cyber-threats. Moreover, this chapter has yielded a key insight; the understanding that the cyber security frameworks and strategies are not binding but voluntary. As a result, it can take quite some time, or even be impossible, to implement the proposed measures in every member state. As a result, on the one hand, this development reduces the internal validity of the report since the outcomes are biased. On the other hand, since these measures are assumed to be partly and slowly implemented throughout the EU, policy proposals, as a result of this thesis, can be implemented in an earlier stage to reduce excessive costs, yet improve the ability to deter.

4. Analysing cyber deterrence in the EU

This paragraph seeks to perform twofold tasks in order to establish enough knowledge and understanding of the European cyber security framework, in relation to cyber deterrence theory, to answer the research question. First of all, it will use Goodman's variables, as noted in table 1, to scrutinise the European cyber security framework. The measures that have been established or proposed in the European cyber security framework that reflect, either directly or indirectly, the cyber deterrence variables in table 1, will be seen as relevant. Other measures will be left out. Secondly, using cyber deterrence scholars' arguments, the strength of these relevant measures, will be assessed. Additionally, three sub-paragraphs have been established which reflect the different clusters within Goodman's cyber deterrence conceptualisation. These sub-paragraphs help narrowing down the search for data and, subsequently, help finding the relevant cyber security measures.

4.1 Europe's formulation of cyber deterrence

This sub-paragraph focusses on the aspects of cyber deterrence that are related to the written formulation of the 'interests' and the 'deterrence declaration' of the Union. These two variables differ to the other cyber deterrence variables since they are not security measures, but 'merely' texts. Therefore, the actual ability to execute and the credibility thereof are not taken into consideration in this sub-chapter.

Starting with the first element of Goodman's cyber deterrence theory; the 'interest' variable relates to anything that the government and/or governance actors see as important and highlight as worthwhile to protect. To this end, the Commission highlights the importance and necessity of CII's (Critical Information Infrastructures) since they are the "ICT systems that are critical infrastructures for themselves or are essential for the operation of critical infrastructures" (Commission, 2005). These infrastructures are important for the functioning of telecommunications, computers, software, internet and satellites. Moreover, CII's are indirectly responsible for electricity, gas and water (ENCS, 2012). Additionally, CII's are important for the business and ICT sectors' development and growth

(Commission, 2009A). Secondly, the Commission adds European principles and areas of interest that need to be protected in the cyber realm. The principles include; fundamental rights, freedom of expression and privacy. The areas of interest are largely of economic interest[13], and the Commission argues that these interests cannot be ensured if not for a safe and secure internet and network systems (Commission, 2013).

To ensure the safety of the Unions interests, the Commission has proposed a 5 pillared 'Strategic Priority System'[14], as the runner-up of the 2009 CIIP action plan[15]. Additionally the Commission, in line with Goodman's conceptualisation, has formulated two explicit 'deterrence declarations'; regarding cybercrime:

> *"If the incident seems to relate to a crime, Europol/EC3 should be informed so that they – together with the law enforcement authorities from the affected countries – can launch an investigation, preserve the evidence, identify the perpetrators and ultimately make sure they are prosecuted"*
>
> *(Commission, 2013)*

And state-sponsored cyber-attack:

> *"If the incident seems to relate to cyber espionage or a state-sponsored attack, or has national security implications, national security and defence authorities will alert their relevant counterparts, so that they know they are under attack and can defend themselves… A particular serious incident or attack could constitute sufficient ground for a Member State to invoke the EU solidarity clause"*
>
> *(Commission, 2013)*

For the first time the Union has explicit deterrence declarations. The deterrence declaration for cybercrime ensures that if one commits a crime, he/she will be caught and penalised in accordance with (in most cases) the Council Convention on cybercrime. Not in all cases because the Council Convention on Cybercrime has not yet been ratified by all MSs (Commission, 2013). On the other hand, when a state-sponsored cyber-attack is serious enough, the EU has formulated to collective respond to the threat under article 222 TFEU. However invoking article 222 TFEU is not necessarily a serious threat to potential aggressors, since it is not explicit about what the specific means are that it will use. On the other hand, it does state that everything will be done in order to avoid the threat. This has implications for the credibility and reassurance measures in terms of state-sponsored cyber-attacks. Moreover, although this is the first explicit deterrent message that the EU has formulated, to make cyber deterrence possible, Guitton argues that continuous deterrent messages should be made explicit (2012).

4.2. Europe's ability to execute the deterrence declaration

This sub-chapter focusses on the cyber deterrence elements regarding the ability to execute the prior established deterrence declarations. The execution of the deterrence declaration can be done in terms of 'denial measures' and 'penalty measures'. The former being defensively orientated, whilst the latter is offensive oriented.

'Denial measures' are measured in terms of 'prevention' (i.e. denying a breach) and 'futility' (i.e. denying a successful breach's desired effect). With regard to the denial measures variable, the (proposed) European cyber security framework contains a variety of measures that can be typified in five categories: First of all, the establishment and/or enhancement of institutions on national or supranational scale[16], these include amongst others, the EDA (European Defence Agency) and national CERTs (Cyber Emergency Response Team). Secondly, the establishment and/or enhancement of protocols and systems[17], these include EISAS (European Information Sharing and Alert System) and DRPs (Disaster Recovery Programs). The third category entails the establishment and/or enhancement of frameworks and institutions to enhance cooperation amongst different actors and institutions[18]. To this end, ENISA (European Network and Information Security Agency) and EP3R (European Public Private Partnership for Resilience) are important, yet diverse, institutions. The fourth element entails the establishment and/or enhancement of (incentives for) programs to raise the ability and awareness across public, private and military actors[19]. It includes MSs raising awareness by introducing a 'cyber security month', industries raising awareness and European institutions such as ENISA to enhance the competence of IT professionals. Finally, the EU uses its knowledge and capital to invest in the establishment, improvement and the instrumentation of third countries' cyber security platforms[20]. Moreover, each of these measures has its specific function in the European cyber security model[21].

The European cyber security framework has very limited resources to prevent cybercrimes. The reason for this is that the framework and strategies seek to protect CII's, whilst cybercriminals often target end users. As a result, the measures are perhaps able to effectively prevent an attack on CII's, but are unable to prevent the breach of an end users computer or private infrastructure. However, the investment in third country cyber security frameworks reduces the ability of criminals of third countries to breach European citizens' infrastructures. International cooperation has been highlighted by many cyber deterrence authors as key to cyber deterrence e.g. (Goodman, 2010; Lan et all, 2010). Moreover, the European awareness campaigns can improve the general safety of end users and make it less likely that they are victimised by cybercriminals. To this end, Cullifo et all argue that increasing the general safety of the end users will function as an 80% solution to the general cyber-threats, the freed up capital and resources could then be invested in more complex cyber-threats (2012), including state-sponsored cyber-attacks. In terms of the prevention of state-sponsored cyber-attacks, the European institutions, cooperation platforms and protocols seek, and are able, to prevent state-sponsored cyber-attacks or any cyber-threat aimed at CII's. Raising awareness, in this context, helps reducing the chance that end users' computers are used in botnets[22]. Moreover, investing in third countries' cyber security framework can reduce the threats of state-sponsored cyber-attacks since they might be less willing to aggress.

In terms of the 'futility' indicator, the European cyber security framework is, to some extent, able to render state-sponsored cyber-attacks entirely futile. The DRP[17] (Data Recovery Program) provides for the means to re-engage CII's, whilst other institutions like the CERTs are able to mitigate the actual attacks. Another means to mitigate state-sponsored cyber-attacks, or render them futile, is international cooperation. On this subject, Goodman's findings in applying the cyber deterrence theory to the Estonian case of 2007 yielded the insight that international cooperation aided in the mitigation and recovery of the cyber-attacks. Moreover, Goodman's findings in Estonia entailed the insight that cyber-information could be endlessly copied, and thus made attacks futile (Goodman, 2010). However, although the attacks can be rendered futile, damages are still applied. Moreover, as a result of an attack, the CII's can be down for a period of time. This down-time may result in high costs depending on the type of infrastructure attacked. To this end, the deterrence of a cyber-attack is crucial. Rendering cybercrimes futile, on the other hand, requires perpetrators to be found first. The costs imposed by the perpetrator can then be revoked according to (inter) national law. To this end, the futility measure is very dependent on the 'reassurance' variable which will be analysed in 4.3.

'Penalty measures' are the offensive aspect of the deterrence declaration, they are measured in terms of 'retaliation' (attacking an aggressor back to impose costs and damages), 'interdependency' (mutual interests that will be negatively influenced in case of a cyber-attack) and 'counter productivity' (retaliating against an aggressors strategic goal, after he/she has succeeded in a tactical goal). Starting with 'retaliation', the measures provided for by the strategic priority plan and the CIIP action plan, that were meant for the protection of CII's[16-20], can be used for offensive measures as well. Moreover, the cyber security strategies have proposed specific measures related to the attribution of aggressors[23], both criminal and state-sponsored. These measures include the cooperation between MS's law enforcement agencies, EC3 and CEPOL. With these proposed measures, Europe's ability to attribute a perpetrator seems strong.

The next step contains the question how to retaliate and whether or not retaliation is legal. Additionally a distinction must be made between state actors and non-state actors. Non-state actors cannot be retaliated against since they have no identifiable infrastructure to retaliate against (Geers, 2010). Moreover, there are no legal provisions which allow a state to attack a person, only legal guidelines to punish a person. These provisions are signed by the majority of the MSs under the Council Convention on Cybercrime. Retaliatory measures against state actors, on the other hand, must be in line with article 2(4) of the UN charter (O'Connel, 2012). Article 2(4) states that when the security of a state comes under threat, self-defence is justified if paired with reasonable, necessary and proportionate measures. However states may only retaliate when the attack by the aggressor reaches the level of an armed attack (Shackelford, 2009). A state-sponsored cyber-attack alone would thus not invoke article 2(4), and retaliation is not an option if a state really wants to act according to international legal provisions. To this end, the Commission, in its latest communication, has formulated a declaration that suggests enabling retaliation under the solidarity clause; article 222 TFEU. The solidarity clause states that any means will be used to prevent an attack on European states. Since the notion of 'any means' is quite vague, it could possibly entail pre-emptive attacks to disrupt the aggressing state-actors' capacities to attack CII's or other targets. The uncertainty concerning the specific measures leaves the strength of this variable in ambiguity, however, it is certain that anything will be done to prevent the attack. Scholars warn for the use of retaliatory measures since they can have unexpected consequences. An example is the 'Stuxnet' virus of which 40% was 'misfired'; targeting innocent third party computers. The retaliatory measures, then, are difficult due to complexities of attribution, and in terms of cybercrimes impossible due to international legal provisions.

The penalty measure variable consists of two additional indicators, besides retaliation, namely: 'counter productivity' and 'interdependency'. In terms of the first indicator, the data has not provided for an indication of the state's ability and/or willingness to understand the perpetrators' strategic goals. Not knowing this goal renders retaliation under the 'counter productivity' indicator impossible. As a result, this indicator will be left out. Conversely penalty by 'interdependency' is an indicator that is maximized by the EU. Europe's socio-economic and political power enables it to invest and trade with many foreign countries[24]. These investments make the countries receiving them dependent on the EU, lowering their willingness to aggress (Goodman, 2010). Moreover, Europe's willingness to invest in third-country cyber security frameworks further enhances this (inter)dependency. However, although the EU creates these (inter) dependencies with state actors; it is difficult to assess its implications on non-state actors, since they do not directly benefit from these mutual agreements. So, on the one hand this indicator is maximized, whilst on the other it his highly ambiguous. However the amount of cybercrime, relatively to the amount of state-sponsored cyber-attacks, indicates that perhaps interdependencies do not have an effect on individuals in the cyber-realm. However further research is required to conclude anything with certainty.

4.3. Europe's ability to ensure the deterrence declaration

This sub-chapter seeks to analyse the 'credibility' of the denial and penalty measures, as well as the 'reassurance' of the deterrence declaration. The former reflects Europe's ability and willingness, from the aggressor's perspective, to apply the denial and penalty measures. The latter relates to the reassurance that an aggressor has that his action will lead to the written reaction by Europe, both from a criminal and state-sponsored perspective. This sub-chapter also contains the remaining variables that were not measurable using the chosen datasets; 'fear' and 'cost benefit calculation'.

The 'credibility' of the EU is measured in terms of the ability and willingness to execute the deterrence declaration. The ability of the EU to execute both its denial and penalty measures to ensure the deterrence declaration, can be found in cyber security framework strategies[16-20,23]. The deterrence declaration, highlighting article 222 TFEU, stresses Europe's willingness to apply the means necessary to defend its interests against state-sponsored cyber-attacks. However, to refer back to a point mentioned under the 'retaliation' indicator, the Commission has formulated its willingness to retaliate against possible perpetrators under article 222 TFEU. The credibility of the EU is strengthened by article 222 TFEU due to its formulation. The use of the notion 'any measures' creates a high level of credibility. To this end, 'any means' can mean anything, including doing nothing. Subsequently, since the credibility measure looks at the ability and willingness to e.g. do nothing, the action is seen as credible. Thus, rather than explaining in specific what the European response to a cyber-attack will be, the EU seeks to keep these measures a secret, creating a fake sense of credibility within Goodman's conceptualisation. Conversely, cyber deterrence scholars argue that not formulating specific cyber defence/offence capabilities, deprives potential aggressors of the ability to copy or bypass these means (Lan et all, 2010), ultimately strengthening the ability to deter. To this end, the EU does use the media and scholarly writings as sources to reach out to potential aggressors, showing off its capabilities without giving any details. An example is the ENISA "key findings" report on the EU-US cyber-exercise (2012). This exercise had considerable scholarly and media attention globally[25] and adds to the credibility of the European cyber-security framework.

In terms of cybercrimes, the Council convention on Cybercrime and national regulation concerning cyber-crimes, highlight the legal measures set in place. These measures, together with the institutions upholding them, give evidence the European willingness to apply the cyber security strategies to ensure the deterrence declaration. However, these measures are to penalise a cybercriminal for his act, they have limited ability to deny an attack and very limited ability to retaliate against one. All in all, from the perspective of adversaries, the ability and willingness of the EU to apply their denial measures against state-sponsored cyber-attacks is very strong and historically proven e.g. Estonia or Georgia. Conversely, in terms of cybercrime, the EU has very limited ability, yet strong willingness, to actually deny a criminal act. However, measures are taken, e.g. raising awareness, to reduce the amount of cybercrime by protecting the end users. In terms of penalty measures, the EU has very little/no ability to retaliate against individuals, both legally and theoretically. Legally it is only allowed to punish them according to their crimes under the Council Convention on Cybercrime, whilst theoretically it is impossible to retaliate against cybercriminals because they have no identifiable infrastructure to retaliate against (Geers, 2010). Conversely, the EU has opened up the legal possibility, under article 222 TFEU, to retaliate against state-sponsored cyber-attacks. however, retaliation can be done using conventional measures or cyber-measures, and especially the latter provides for problems concerning the proportionality of the attack (O'Connel, 2012). To this end, retaliation may still be against international legal provisions. Hover, even if the retaliatory measure is proportionate, it will be against article 2(4) of the UN treaty.

The reassurance variable reflects the level of certainty a potential aggressor has that an attack would lead to an appropriate measure by the defender, as stated in the deterrence declaration. The deterrence declaration regarding cybercrimes states that cybercriminals will be found and prosecuted. To this end, national and supranational law enforcement agencies[21] are tasked with the attribution of criminals. The prosecution of the perpetrators is mostly done on the basis of the Council Convention on Cybercrime. Additionally, the Commission has proposed other means to increase the ability and effectiveness of attribution[26]. However, do these measures really reassure a potential aggressor that if he does X, the Union will respond by doing Y? Guitton believes not, his study pointed out that merely a fraction of all cybercriminals are caught and penalised in the three countries he based his research on[27]. Similarly, other authors argue that attribution is very difficult (Goodman, 2010; Cullifo et all, 2012). Attribution is made difficult because hackers are able to remotely access other computers and use them to commit crimes or attack infrastructures. Moreover, when the actual perpetrators are caught, they can argue that they were not the source of the attack, but that their computer was hacked as well. This is called 'false flagging' (Goodman, 2010; Geers, 2010). However, all in all, the new attribution measures improve, to quite some extent, the ability to reassure the deterrence declaration. Although the extent of the improvement depends on the technological development of the MSs, the cybercriminals and the extent to which the Commissions strategy is implemented by the MSs.

The reassurance of Europe executing its deterrence declaration, in case of a state-sponsored cyber-attack, is ambiguous. The attacks on Estonia that took place over a period of two weeks, which nearly collapsed the entire Estonian CII, led to the penalisation of a Russian student with $ 1.642,-. Although the penalty for his crime in particular is proportionate, the amount of damages dealt to the Estonian infrastructures were not compensated for. Moreover, although the EU did not have an explicit deterrence declaration during that timeframe, its full capabilities were not sufficient to prevent the attacks. Moreover, after the attacks on Estonia in 2007, the Estonian authorities were unable to find and penalise the perpetrators for two reasons. First of all, attribution proved to be a problem; where the attacks originated from IP-addresses from the US, the actual perpetrators were thought, and found, to be living in Russia. Secondly, the refusal of the Russian grand court to provide cooperation after the Estonian request for a bilateral investigation under MLAT (Mutual Legal Assistance Treaty) made the investigation difficult and required extra time and resources. Although since the attacks on Estonia, the European cyber security framework has improved dramatically in terms of CERT capabilities, international cooperation and digital forensic tools, it does not make the attribution easier when the nation state from which the attacks are thought to originate refuses to collaborate. To this end, Goodman argues that even if the actual attacks were not state-sponsored, international law should be updated to hold the state liable for where the attacks came from. As a result, protecting those who are liable, by e.g. not cooperating, would mean being liable as a state (2010), making attribution much easier.

Thus far, the measures that have been analysed include European means to attack, defend and the credibility thereof. However, there are two variables in Goodman's cyber deterrence conceptualisation which could not be measured using the selected datasets. The first variable; 'fear' reflects the fear that has been put, using other cyber deterrence variables e.g. deterrence declaration and penalty measures, into the adversaries eyes. To this end, 'to fear' something is not necessarily 'to be deterred from', rather, fear is a factor that plays a role in enabling a person to deter or to be deterred. The second variable is; 'cost-benefit calculations', this variable seeks to identify whether or not the applied cyber security measures are cost-benefit friendly. To this end, cost-benefit friendly measures improve the ability to deter potential adversaries (Goodman, 2010).

Starting with the variable fear, although fear is implied in almost all cyber deterrence conceptualisations, the measurement thereof is rather ambiguous considering that first of all, one can argue that those that aggress against the European cyber security framework, have no fear thereof. On the other, hand scholars argue that (cyber) crimes are based on impulses rather than logical decisions (Goodman, 2010), making fear unnecessary as a measure in terms of cybercrime. Moreover, can it be concluded that those who do not attack the European cyber security framework are fully feared by the framework? Or are they just non-criminal? Fear is implied in most cyber deterrence theories, yet not made explicit and measured. To this end, this thesis argues that although Goodman's conceptualisation of cyber deterrence was the most comprehensive and realistic approach to cyber deterrence, the variable fear should play a different role in it[28]. All in all, there is no evidence, nor data, to apply the variable 'fear' on the European cyber security framework, therefore it will be left out.

Similarly to the variable fear, the variable 'cost-benefit calculation' will be left out; first of all, because there are no data on the exact costs of cybercrime or state-sponsored cyber-attacks, or on the benefits of cyber security measures. Secondly, the data that has been made explicit are often based on estimates and thus invalid. All in all then this variable could not be measured with the existing data-sets. However, scholars assume that any costs made, to refrain a potential aggressor from attacking, outweighs the costs endured when a critical infrastructure is down for even a short period of time (Goodman, 2010). Moreover, this thesis argues that the actual ability to be cost-benefit friendly has little to nothing to do with the ability to refrain a potential aggressor from attacking; rather it has implication on the decision, whether or not, to apply a cyber deterrence policy. To this end, this thesis argues that cost-benefit calculation is not a valid variable for measure cyber deterrence.

This paragraph has sought, as a step towards answering the research question, to analyse the extent to which the European cyber security framework reflects the elements of cyber deterrence theory, as conceptualised by Goodman (2010). This quest has yielded the key insight that Europe's cyber security framework reflects all necessary cyber deterrence conditions. The presence of these required cyber deterrence elements allow for a valid conclusion to be drawn in the final paragraph. To this end, the findings of this paragraphs portrayed a very willing and capable Europe, both in terms of denial and penalty measures. However, although article 222 TFEU is the backbone of the deterrence declaration vis-à-vis state-sponsored cyber-attacks, article 2(4) of the UN charter potentially clashes with the execution thereof. A similar clash arose with the Kadi case law[29] which was eventually won by the EU. With regard to cybercrime, Europe's abilities to attribute and prosecute are significantly improved with the establishment of the EC3 and the already signed Convention on Cybercrime. Conversely, Europe's ability to deny, or retaliate against, a cybercrime has proven impossible. First of all the sheer amount of crimes does not allow for an institutional response, rather the EU seeks to raise awareness amongst end users in order to prevent cybercrimes. In terms of retaliation, the EU has no legal provision that allows attacking a citizen in order to impose costs that outweigh their benefits of cybercriminal activity. These findings negatively influence Europe's ability to deter with regard to the specific cyber threat. Moreover, two variables proved immeasurable using the selected datasets; 'fear' and 'cost-benefit calculation'. These variables have been left out and are not taken into account in the conclusion. Nevertheless, the presence of the variables, especially ‘fear’, can be assumed if the framework is able to deter an adversary (Goodman, 2010). Finally, of these two variables, the ‘cost-benefit calculation’ has been argued as irrelevant for the actual ability to deter a cyber-threat. Moreover, the variable fear should either be conceptualised differently, or left out altogether, to avoid an omitted variable bias. This re-arrangement will not affect this thesis because the variable fear was immeasurable and left out altogether, however it is an important consideration for future cyber deterrence conceptualisations.

5. Conclusion

The search to apply cyber deterrence theory to the European cyber security framework, in order to assess its ability to deter, has led to various insights, findings and policy proposals. To this end, the insights that have been obtained are; first of all, that it seems as if Europe has implemented changes on the basis of the lessons learned from, above all, Estonia. Finding the source of the attacks and the people responsible proved impossible in the aftermath of the cyber-attack on Estonia. The changes that have been put in place mostly aim at increasing awareness to reduce cybercrimes and improving forensic tools to attribute aggressors, both state and non-state actors. To this end, the EC3 has been established as a key tool for improving attribution. Secondly, the insight has been obtained that international agreements are likely to be overruled during and after a state-sponsored or state-involved cyber-attack. This insight is based on the Estonian cyber-attack case, where Russian authorities were unwilling to cooperate under the MLAT treaty to assist Estonian research to attribute the perpetrators. Conversely, other international treaties should either no longer be upheld or be updated in order to meet the need for international law regarding state-sponsored cyber-attacks. The EU has updated their laws by applying the existing solidarity clause to serious cyber-threats. Conversely, the UN, of which a majority of MSs are members, is lagging behind in terms of establishing international laws that reflect cyber-threats. Thirdly, cyber deterrence theory measures the ability to deter an adversary from aggressing towards an interest. To this end, cyber deterrence is more applicable and fosters more relevant outcomes if applied to adversaries such as terrorists or nation states; actors that seek to invoke damages to infrastructures. Cybercriminals, much like conventional criminals, are not easily deterred, if anything, cybercriminals are much harder to deter due to the sheer amount and the difficulties concerning the attribution of them. Nevertheless, the findings of this thesis on cybercriminals are still relevant since the policies to deter them similarly apply to the deterrence of cyber-terrorists (Bendiek, 2012).

Summarizing all the cyber deterrence variables Goodman proposed[30], the following answers can be given to the research question: ‘*to what extent is the European cyber security framework able to deter cyber-threats?*’ In terms of cybercrimes, the European cyber security framework has very limited ability to deter cybercrime. The main reason for this is the lack in denial by prevention and penalty measures in general. Another reason could be the argument that crime is not based on logic, but instincts and emotion (Goodman, 2010). As a result, cybercriminals cannot be deterred since deterrence theory assumes perfect information and logic. Conversely, Bendiek argues that measures against cyber-terrorists similarly affect cybercriminals. This suggests that cybercriminals, like cyber-terrorists, use logical reason and arguments for their actions. Unfortunately the findings of this thesis do not support any of the arguments, nor does it refute them. All in all, the European cyber security framework has limited ability to prevent cybercrimes and no ability to (legally) retaliate, but it is very capable in the attribution and subsequent prosecution of cybercriminals.

The variables that, according to Goodman's framework, have to be improved are the denial by prevention, penalty by retaliation and penalty by interdependency in order to improve the ability to deter. In terms of denial by prevention, Will Goodman argues that a means should be established to prevent cybercriminals from committing a crime. Conversely, the EU seeks to prevent cybercrimes by raising awareness amongst the public to protect themselves. This makes the EU very dependent on the moods, visions and budgets of the European citizens to protect themselves. This thesis argues that Goodman's solution is not practical because of the sheer amount of cybercrimes that need to be prevented. Similarly, the European solution is not effective enough. Alternative measures to prevent cybercrimes by improving end users' protection are to; first of all, creating incentives to buy (high-end) cyber-security programs by reducing the tax on these products[31]. Cullifo et all would support this argument and add that improving the basic security of end-users would be as much as 80% of the solution (2012). The second proposal is to approach the private cyber-security corporations and legally oblige them to cooperate, to some extent, to fulfil their share of the task in protecting end-users[32]. A similarity can be drawn between how countries like the Netherlands treat the private companies regulating the railroad infrastructure, and how this thesis proposes Europe to treat the private companies that regulate the information infrastructure.

In terms of the penalty by retaliation measure, the findings of this thesis contradict the possibility of the developments required by Goodman's conceptualisation of cyber deterrence. There are no legal grounds to which governments can be enabled to attack private infrastructures in order to impose costs. Although some plans exist to do so something seemingly similar (NOS, 2013), these developments are uncertain in legal terms. In terms of the penalty by interdependency indicator could perhaps be improved, yet the findings of this thesis do not support, nor reject the possibility thereof. More research and theorisation is required for such a conclusion to be validly drawn. All in all, the absence of these measures may lead to Europe remaining unable to deter cybercrimes. However, Europe should not lose its democratic values in the fight against cyber-threats. For example, if you would Google NSA, you will find numerous websites and news items related to the NSA tapping phones and other means of communication. Western societies are expressing their disapproval of such actions. Similarly, Bendiek argues that in the face of these cyber-problems, Western societies have opted for security over core democratic values; she calls this problematic development 'securitisation' (2012)[33]. These developments are anti-social and destroy the core rights and freedoms for which the Union and democracy stand. Harnessing and applying these abilities would make governments just as much as a threat for their citizens as cyber-criminals and cyber-terrorists.

The second type of cyber-threat which thesis has sought to assess Europe's deterrence capabilities for is; state-sponsored cyber-attacks. Europe is much more capable of deterring state-sponsored cyber-attacks. Better still, the European cyber security framework scores between strong and very strong on all measurable variables and indicators. As a result, the European cyber security framework, once fully established, allows for a strong ability to deter state-sponsored cyber-attacks. If a similar attack to Estonia would occur, the costs as a result of damages would be very small and the aggressors will have smaller chance of escaping. This is unless the adversary's government decides to obstruct the attribution process by ignoring international treaties. To this end, two policy proposals tackle this problem. First of all, Europe should seek to establish international treaties with every single nation state for the cooperation in the search, extradition and prosecution of cybercriminals. This can be done via UN provisions or even 'bilateral' between the EU and third parties. This proposal is to increase Europe's ability to attribute and prosecute a perpetrator in general. Secondly, in order to ensure the preservation of those treaty, international treaties have to be established, within the UN or bilaterally, which holds the country from which the attack commenced liable unless the actual perpetrator is found. Goodman has proposed this as a result of his cyber deterrence research in Estonia and Georgia; he adds that this measure will ensure the cooperation of other countries. Moreover, if the state refuses to cooperate, it does not matter since the costs endured can be claimed from the state instead of the actual perpetrator. Moreover, retaliatory measures against such a state could be approved, effectively deterring them of refusing to cooperate.

Cyber deterrence theory seems to be relatively more fit to apply to state-sponsored cyber-attacks than cybercrimes. Although not explicitly, it seems that Will Goodman has implicitly used a nuclear deterrence analogy for cyber deterrence. Conversely, O'Connel has argued that maximizing a nuclear deterrence analogy will not lead to a safer cyberspace (2012). Other analogies[3] should be applied to more specifically reflect the cyber-threat that requires deterrence. The findings of this thesis support O'Connel in the argument that different analogies, and therefore conceptualisations, should be applied to different type of cyber-threats. However, there are no findings supporting the argument that nuclear deterrence yields unfavourable results in terms of cyber security.

Finally, the implications of the insights and conclusions yield some worrying discoveries. First of all, the inability of Europe to deter cybercriminals results in the continuation of the high level of cybercrimes in Europe. Unless the EU is able to attribute and prosecute these criminals, they will continue to attack private infrastructures for their own benefits. Alternatively the EU could improve the protection of end-users by increasing awareness and creating incentives by reducing taxes. However, Guitton would argue that these improvements are short term and will result in the continual attempt of criminals until they are found and prosecuted. To this end, the establishment of the EC3 is a milestone in Europe's deterrence abilities; however its full competencies are required. Secondly, if Bendiek is right when arguing that cybercriminals and cyber-terrorists are deterred in the same way, it is possible that in the near future major cyber-terrorist attacks will be executed. Moreover, unless Europe improves their ability to attribute, these attacks, according to Guitton, will continue for as long as they want and can. To this end, Goodman's proposal for state liability in case of a cyber-attack is a valuable measure to ensure international cooperation and therefore the attribution of cyber-terrorists. All in all, it is clear that cyberspace is the fifth domain of warfare (Furgeson and Mansbach, 2012). Cyber deterrence is an effective response to these new threats, however, when ensuring the ability to deter potential adversaries, the EU should not forget their core values and the rights of its citizens.

6. References

Beth, M. (2008). *A Nuclear weapon-free world is possible, Nunn say*. Belfer Center, Harvard University.

Bendiek, A. (2012). *European Cyber Security Policy.* SWP Research Paper. Berlin.

Carr, J. (2012). *Inside Cyber Warfare: Mapping the Cyber Underworld*. O'Reilly Media Inc. USA.

Clapper, J.R. (2013). *Worldwide Threat Assessment of the US Intelligence Community.* Senate Select Committee on Intelligence.

Clarke, R.A., Knake, R.K. (2010). *Cyber War: The Next Threat to National Security and What to Do About it.* Harper Collins.

Commission. (2005). *Green Paper on a European Programme for Critical Infrastructure Protection*. Brussels

Commission. (2009A). *On Critical Information Infrastructure Protection*. Brussels.

Commission. (2009B). *Protecting Critical Information Infrastructures: Frequently Asked Questions*. Memo/09/141. Brussels

Commission. (2013). *Cybersecurity Strategy of the European Union: an open, safe and secure cyberspac*e. Brussels.

Cullifo, F. J., Cardash, S.L., Salmoiraghi G.C. (2012). *A Blueprint for Cyber Deterrence: Building Stability Through Strength*. Military and Strategic Affairs Volume 4 (3).

Derene G. *Weapon of mass disruption*. Popular Mechanics 2009; 186(4).

ENCS. (2012). *Securiting Europe's Critical Infrastructures*. The Hague, The Netherlands.

ENISA. (2012). *Cyber Europe 2012: Key Findings and Recommendations*.

Feaver, P.D. *Blowback*. Security studies 7, no 4.

Fukuyama, F. (1992). *The end of history and the last man*. Free press. ISBN 0-02-910975-2.

Furgeson, Y.H., Mansbach, R.W. (2012). Globalization *The Return of Borders to a borderless world?* Routledge.

Geers, K. (2010). *The Challenge of Cyber Attack Deterrence.* Computer Law & Security Review 26. Elsevier.

Gibbs, J. P. (1985). *Deterrence Theory and Research.* Nebraska Symposium on Motivation. The Law as a Behavioral Instrument (Vol. 33). Lincoln: University of Nebraska Press.

Goodman, W. (2010). *Cyber Deterrence Tougher in Theory than in Practice*? Strategic studies Quarterly.

Guitton, C. (2012). *Criminals and cyber attacks: the missing link between attribution and deterrence*. Internation Journal of Cyber Criminology: Kings college London, UK.

Jacob, H. (1978). *Rationality and Criminality*. Social Science Quaterly, 59(3), 584-585.

Kokot, J. and Sobotta, C. (2012). *The Kadi Case – Constitutional Core Values and International Law – Finding the Balance.* The European Journal of International Law vol.23 no.4. Oxford University Press.
Kugler, R. (2009). *Deterrence of Cyber Attacks*. Washington, D.C.: National Defense University Press

Kshetri, N. (2010). *The Global Cybercrime Industry: economic, institutional and strategic perspectives*. Springer

Lan, T., Xin, Z., Raduege, H.D., Grigoriev, D.I., Duggal, P., Schjolberg, S. (2010). *Global Cyber Deterrence: views from China, the U.S., Russia, India and Norway*. EastWestInstitute, New York.

Long, A. (2008). *Deterrence: From Cold War to Long War*. Santa Monica.

Nagin, D.S. (2011). *Deterrence: Scarring Offenders Straight*. Correctional Theory: Context and Consequences. Sage publications.

NOS. (20130. *Opstelten: wet voor terughacken*. http://nos.nl/artikel/502354-opstelten-wet-voor-terughacken.html

O'Connel, M.E. (2012). *Cyber Security without Cyber War*. Journal of Conflict & Security Law. Oxford University Press.

Pendall, D.W. (2004). *Effects-based operations and the exercise of national power*. Military Review; 84(1).

Pratt, T. C., Cullen, F. T., Blevins, K. R., Daigle, L. E., & Madensen, T. D. (2006). *The Empirical Status of Deterrence Theory: A Meta-Analysis*. The Status of Criminological Theory. New Brunswick: Transaction Publishers

Prins, R. (2012). *Een veilige cyberwereld vraagt nieuw denken*. Justitiële verkenningen, jrg. 38, nr. 1, 2012 Veiligheid in Cyberspace. Boom Lemma uitgevers.

Schmidt, A. (2012). *At the boundaries of peer production: The organization of internet security production in the cases of Estonia 2007 and Conficker*. Elsevier.

Shackelford, S.J. (2009). *Nuclear War to Net War: Analogizing Cyber Attacks in International Law*. Berkeley Journal of International Law.

Waxman, M.C. (2011). *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4).* The Yale Journal of International Law [Vol. 36].

Wheatley, G.F., Hayes, R.E. (1996). *Information Warfare and Deterrence*. Washington: NDU Press.

Wilson, C. (2008). *Botnets, Cybercrime, and cyberterrorism: Vulnerabilities and Policy Issues for Congress*. Congressional research service.

Zimmerman, J. (2013). *A Theory of Cyber Deterrence*. Georgetown Journal of International Affairs. http://journal.georgetown.edu/2013/02/06/a-theory-of-cyber-deterrence-christopher-haley/

1 – Definition cybercrime

Scholars like Krone suggest that cybercrime is criminal activity against data and copy right (2005). Hovever, scholars like Zeviar-Geese suggest that cybercrime is not only related to criminal activity against data and copyright, but also fraud, cyber-stalking and child pornography (1998). A more recent scholarly conceptualization by Clay Wilson defines cyber-crime as “crime that is enabled by, or that targets computers” (2008). Wilson mentions aspects such as theft of IPR’s (Intellectual Property Rights), violations of patents or copyright laws, but also unauthorized access to computers and the deliberate disruption of computers for e.g. espionage (2008).

2 – Identified types of cybercrime by Council Convention on Cybercrime

The Council Convention on cybercrime defines the following cybercriminal activities:

1) Offenses against the confidentiality, integrity, and availability of computer data and systems;

- Illegal access
- Illegal interception
- Data interference
- System interference
- Misuse of devices

2) Computer-related offenses;

- Computer-related forgery
- Computer-related fraud

3) Content-related offenses;

- Offences related to child pornography

4) Offenses related to infringements of copyright and related rights.

- Offences related to infringements of copyright and related rights

Source: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

3 - Deterrence

Deterrence theory itself dates back to the Peloponnesian war (Long, 2008). Under scholars such as Thomas Schelling (1966) it gained significant momentum. However, it wasn't until the cold war where, under the threat of MAD (Mutually Assured Destruction), deterrence theory showed its full potential. During this era both USSR and US were deterred from aggressing towards each other since they both knew that the other side had the ability to counter the initial attack with equal or more severe retaliation measures (Geers, 2010). The success of mutual deterrence in this domain has caused scholars to try to apply the cold war deterrence analogy to the cyber domain, however other analogies exist as well[3]. Superimposing deterrence to the cyber domain creates: 'Cyber deterrence' (Lan et all, 2010; Guitton, 2012; Goodman, 2010; Geers, 2010; Cullifo et all, 2012; Connel, 2012; Weiner, 2012). However, these scholars use different definitions and conceptualisation of the concept cyber deterrence. The next paragraph will explain these differences and highlight the disagreements from the perspective of three key authors.

4– Article 2(4) UN

The Organization and its Members, in pursuit of the Purposes stated in Article 1, shall act in accordance with the following Principles.

4. All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.

Source: http://www.un.org/en/documents/charter/chapter1.shtml

5 - Article 222 TFEU

1. The Union and its Member States shall act jointly in a spirit of solidarity if a Member State is the object of a terrorist attack or the victim of a natural or manmade disaster. The Union shall mobilise all the instruments at its disposal, including the military resources made available by the Member States, to:

(a)

– prevent the terrorist threat in the territory of the Member States;

– protect democratic institutions and the civilian population from any terrorist attack;

– assist a Member State in its territory, at the request of its political authorities, in the event

of a terrorist attack;

(b)

assist a Member State in its territory, at the request of its political authorities, in the event of a natural or man-made disaster.

Source: http://www.eudemocrats.org/fileadmin/user_upload/Documents/D-Reader_friendly_latest%20version.pdf

6 - Council Convention on Cybercrime

Source: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

7 – EC3

The EC3 (European Cyber Crime Centre) was officially established within EUROPOL on the 1st of January 2013 with the following mandate in the area of cybercrime:

- To (help) fight organised cybercriminal groups that make large profits
- To (help) fight cyber-threats that cause particular serious harm
- To (help) fight cyber-threats that affect critical information infrastructures in the EU

Source: https://www.europol.europa.eu/ec3

8 – EUROPOL

Europol is the Unions law enforcement agency. With about 800 persons working in its headquarters in The Hague, it carries out an estimated 13.500 investigations. Its mandate is twelvefold :

- The support and coordination of drugs related investigations
- The support and coordination of human trafficking investigations
- The support and coordination of illegal migration investigations
- The support and coordination of cyber-crime related investigations (under EC3)
- The support and coordination of the investigations of crimes related to IPR's (Intellectual Property Rights)
- The support and coordination of investigations aimed at cigarette smuggling
- The support and coordination of investigations aimed to counter counterfeiting
- The support and coordination of VAT fraud investigations
- The support and coordination of investigations aimed to counter money laundering
- The support and coordination of investigations against MOCG's (Mobile Organised Crime Groups)
- The support and coordination to prevent criminal activities of OMCG's (Outlaw Motor Cycle Gangs)
- The support and coordination with the fight against terrorism

Source: https://www.europol.europa.eu

9 – ENISA

ENISA (European Network and Information Security Agency) has a fourfold (main) tasks, besides smaller functions such as encouraging cooperation between the public and private domains:

- ENISA's CERT (Cyber Emergency Response Team)provides tools and guidelines for MSs to establish and making more effective of CERT's
- ENISA has a special unit that performs several tasks to improve the resilience of CII's (Critical Information Infrastructures) such as:
  - Increasing MS awareness and knowledge
  - Developing good practice guides
  - Organising cyber exercises
  - Co-managing the EP3R (European Public Private Partnership for Resilience)
  - Contributing to the Commission's strategies
- The identity and trust team helps the Commission with the implementation of the Digital Agenda which seeks to raise awareness and trust in various cyber domains

- In the area of risk management, ENISA assesses risk and informs MS experts and non-experts on the (level of) threat. The ultimate aim is to establish a large collection of knowledge related to all sorts of risk for an efficient and better assessment as well as reviewable data collection.

Source: http://www.enisa.europa.eu/

10 – EUROJUST

EUROJUST's goal is described in article 85 of the Lisbon treaty, which formulates EUROJUST's mission as*: "to support and strengthen coordination and cooperation between national investigating and prosecuting authorities in relation to serious crime affecting two or more Member States […]"*

Source: http://eurojust.europa.eu/Pages/home.aspx

11 – ENCS

The ENCS' (European Network for Cyber Security) main task is to secure Europe's Critical Information Infrastructures (CII). To this end, it pools knowledge and resources from and for MSs accessibility. It, furthermore, enhances and facilitates cooperation between public and private actors.

Source: https://www.encs.eu/

12 – EGC

The EGC (European Governmental Cyber Emergency Response Team) is a European based information sharing and cooperation initiative for the various national CERTs. With 11 members to this initiative, the EGC seeks to:

- Develop measures to deal with network security incidents
- Facilitate information sharing
- Identify areas where collaboration, in terms of research, can take place
- Communicate with other organizations and initiatives

Source: http://www.egc-group.org/

13 – Interest variable: areas of interest

- Energy
- Transport
- Banking
- Stock exchanges
- Enablers of key internet services
- Public administrations

Source: (Commission, 2013)

14 – European cyber security strategy: Strategic Priority System

Goals of the Strategic Priority System:

- Achieving cyber resilience
- Drastically reducing cybercrime
- Developing cyber-defense policy and capabilities related to the CSDP (Common Security and Defence Policy)
- Develop the industrial and technological resources for cyber-security
- Establish a coherent international cyberspace policy for the European Union and promote core EU values

Source: (Commission, 2013)

15 – European cyber security strategy: CIIP (Critical Information Infrastructure Protection) Action Plan

Goals of the CIIP Action Plan:

- Preparedness and prevention
- Detection and response
- Mitigation and recovery
- International Cooperation
- Criteria for European critical infrastructures in the ICT sector

Source: (Commission, 2009)

16 – European cyber security measures: the establishment and/or improvement of institutions

The Establishment of:

- The EC3[7]
- ENISA[9]
- ENCS[11]
- EGC[12]
- EDA (European Defence Agency) has the mission to support the Council and the MSs to improve Europe's defence capabilities.

The Commission asks MSs to:

- Establish a competent CERT (Computer Emergency Response Team)
    - CERT's are for handling risks and incidents
    - Define a minimum level of capabilities for national CERTs and incident response operations (implies an increase in competencies and powers of CERTs in terms of capabilities and personnel, this would result in an improved ability to foresee and prevent attacks)
    - Ensure national CERTs as key component for information sharing, coordination and response (this is especially important in the light of supranational and multilateral cooperation in terms of information exchange and thus prevention by means of knowledge on potential threats and sharing this knowledge. Having one national institution at the centre of the national knowledge base makes it easier to acquire knowledge and share it as well)
- Establish a competent NIS authority for
    - Preventing risks and incidents
    - Handling risks and incidents
    - Responding to risks and incidents

Source: (Commission, 2009) & (Commission, 2013)

17 – European cyber security measures: the establishment and/or improvement of protocols

The establishment of Disaster Recovery Programs (DRP's), meant to improve the speed and ability to recover from an infrastructural collapse and the ability to shift resources from one server to the other in order to maintain the attainability of the infrastructure.

Source: http://www.enisa.europa.eu/activities/risk-management/current-risk/bcm-resilience/glossary/c-d

The Establishment of EISAS (European Information Sharing and Alert System) falls within the competencies of ENISA. To this end, EISAS specifies its target groups to citizens and SME's (Small and Medium Enterprises), to whom it shares information on internet security and provides them with the necessary skill and tools to protect themselves.

http://www.enisa.europa.eu/activities/cert/other-work/eisas_folder

Early warning and incident response capabilities are important for a proper assessment of, and response to, the threat. These assessments seek to predict cyber-threats and rely on the well-functioning of nation CERT's.

The Commission asks MSs to:

- Adopt a NIS-strategy (Network and Information Security)

The Commission asks ENISA to:

- Develop a guideline and recommendations for establishing NIS and NIS related standards

Source: (Commission, 2009) & (Commission, 2013)

18 – European cyber security measures: the establishment and/or improvement of cooperation

- The establishment of the 'European Forum' as a means of exchanging information, this provides for a framework of exchange whilst the actors using the framework would be centralised to national CERTs
- Fostering the cooperation between the public and private sector on "security resilience objective" under the EP3R (European Public Private Partnership for Resilience) framework.

The Commission will:

- Establishing cooperation mechanism between the Commission and NIS
    - Means of early warnings on risks and incidents
    - Facilitate exchange of information
    - Facilitate exchange of best practice

The Commission asks the MSs and CSDP to collaborate on:

- Promote dialogue between civilian and military actors to:
    - Raise awareness
    - Establish cybersecurity
    - Establish means of early warning
    - Establish an improved incident response
    - Exchange good practices
    - Exchange information

Source: (Commission, 2009) & (Commission, 2013)

19 – European cyber security measures: the establishment and/or improvement awareness and cyber skill

The Commission asks MSs to:

- Organise a yearly ‘cybersecurity month’
    - Increase awareness of the public
- Enhance national NIS education and training with training on
    - NIS (in schools & public administrations)
    - NIS, secure software and data protection (for IT students)

The Commission asks the industries to:

- Promote awareness “at all levels”

The Commission asks ENISA to:

- Create a roadmap for ‘NIS driving licence’
    - Enhancing skills and competence of IT professionals

The Commission asks the MSs and CSDP to collaborate on:

- Improve cyber training and exercise for the military in Europe
- The DAE (Digital Agenda for Europe), which was adopted in 2010, emphasizes the need for stakeholders to join forces and to ensure security of the critical infrastructures by means of prevention, preparedness and awareness.

Source: (Commission, 2009) & (Commission, 2013)

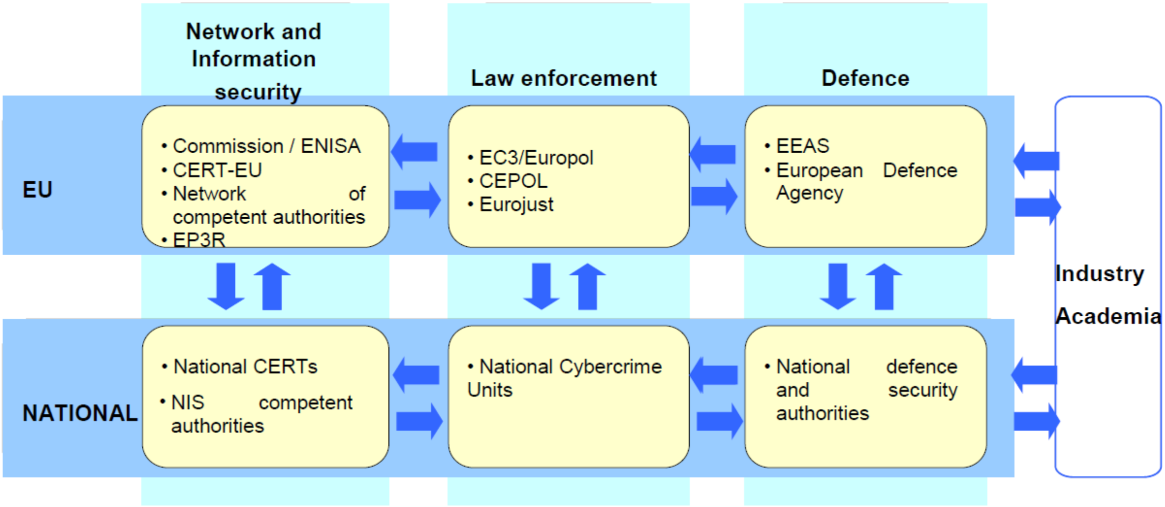
20 – European cyber security measures: the investment in third-countries

The Commission will:

- Support third countries with:
    - Capacity building in terms of cybersecurity and cyber resiliency
        - Training
        - Funding
        - instrumentation

Source: (Commission, 2009) & (Commission, 2013)

21 – The European cyber security model


Network and Information security
Law enforcement
Defence
EU
• Commission / ENISA
• CERT-EU
• Network of competent authorities
• EP3R
• EC3/Europol
• CEPOL
• Eurojust
• EEAS
• European Defence Agency
NATIONAL
• National CERTs
• NIS competent authorities
• National Cybercrime Units
• National defence and security authorities
Industry
Academia

Source: (Commission, 2013)

22 – Botnets

During the attacks on for example Estonia, the main source of damage was the use of so called 'botnets'. These are networks of previously contaminated computers which are activated remotely and receive a task to bomb an infrastructure with requests for information. The result of such an action can be a server overload, resulting in a (temporary) collapse of the server, making it unavailable.

Source: (Schmidt, 2012)

23 – European cyber security measures: attribution

The Commission asks MSs to:

- Identify gaps in terms of investigating and combating cybercrime (funded by EU)

The Commission will:

- Launch a project fighting botnets and malware

The Commission asks the EC3 to:

- Support MSs' cybercrime investigations to:
    - Dismantle and disrupt cybercrime networks
- Closely cooperate with Eurojust to effectively fight cyber-crime

The Commission asks CEPOL to:

- Establish a means of equipping law enforcement agencies with the knowledge to fight cybercrime

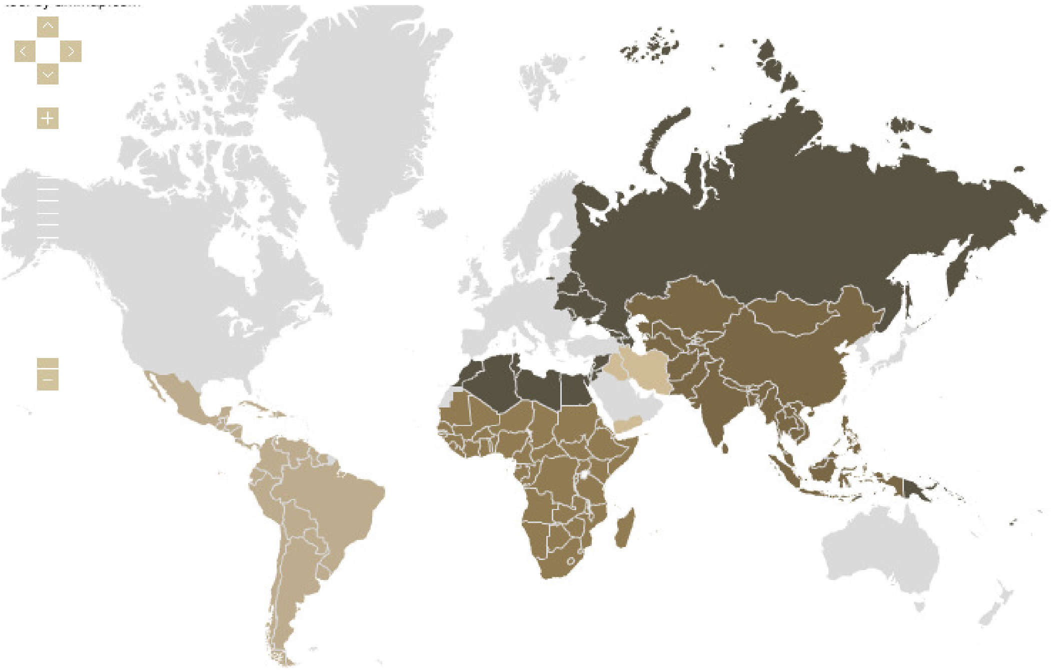
Source: (Commission, 2013)

24 – Europe's international relations

The European investment bank promotes sustainable growth and job creation, within as well as outside Europe, with over a 150 other partner countries. Its investments go to (amongst others):

- Small and medium sized enterprises: the creators of 80% of new jobs
- Regional development: to address economic and social imbalances between regions

The cooperation with countries outside of Europe is done so in line with the provisions of the EU external assistance policy. This external assistance policy is implemented by EuropeAid and the ENP (European Neighbourhood policy) in the following countries:



source: http://ec.europa.eu/europeaid/index_en.htm

"Our Neighbourhood Policy provides us with a coherent approach that ensures that the whole of the EU is committed to deeper relations with all our neighbours. At the same time, it allows us to develop tailor-made relations with each country."
Štefan Füle, Commissioner for Enlargement and European Neighbourhood Policy

For additional information on ENP see: http://ec.europa.eu/world/enp/inadex_en.html

25 – International attention to EU-US cyber exercise

"Cyber Europe 2012 attracted considerable attention in the global media. More than 600 articles were published in 19 languages. Many articles quoted Vice-President of the European Commission responsible for the Digital Agenda, Neelie Kroes, stating that '*Working together at the European level to keep the Internet and other essential infrastructures running is what today's exercise is all about.*' In addition, Cyber Europe 2012 was mentioned in social media in over six languages."

Source: (ENISA, 2012)

26 – European cyber security measures: establishing and improving attribution

The Commission asks MSs to:

- Adopt a NIS-strategy (Network and Information Security)
- Establish a competent NIS authority for
    - Responding to risks and incidents
- Establish a competent CERT (Computer Emergency Response Team)
    - Handling risks and incidents
    - Under the supervision of NIS authority
- Enhance national NIS education and training with training on
    - NIS (in schools & public administrations)
    - NIS, secure software and data protection (for IT students)
- Ratify and implement Council Convention on Cybercrime
- Identify gaps in terms of investigating and combating cybercrime (funded by EU)
- Work closely with EC3 and Eurojust to harmonise policy approaches using best practice.

The Commission asks the industries to:

- Operators of critical infrastructures must report incidents on their services to national NIS authority
    - Liability of reporting incidents lies with the operators

The Commission will:

- Establishing cooperation mechanism between the Commission and NIS
    - Facilitate exchange of information
    - Facilitate exchange of best practice

- Support third countries with:
    - Capacity building in terms of cybersecurity and cyber resiliency
        - Training
        - Funding
        - instrumentation

The Commission asks ENISA to:

- Create a roadmap for 'NIS driving licence'
    - Enhancing skills and competence of IT professionals
- Develop a guideline and recommendations for establishing NIS and NIS related standards

The Commission asks the EC3 to:

- Support MSs' cybercrime investigations to:
    - Dismantle and disrupt cybercrime networks
- Closely cooperate with Eurojust to effectively fight cyber-crime

The Commission asks CEPOL to:

- Establish a means of equipping law enforcement agencies with the knowledge to fight cybercrime

The Commission asks Eurojust to:

- Identify obstacles related to judicial cooperation on cybercrime related investigations
- Coordinate the investigation and prosecution of cybercrime
- Establish training activities for relevant actors
- Closely cooperate with EC3 to effectively fight cyber-crime

The Commission asks the MSs and CSDP to collaborate on:

- Improve cyber training and exercise for the military in Europe
- Promote dialogue between civilian and military actors to:
    - Raise awareness
    - Establish cybersecurity
    - Establish means of early warning
    - Establish an improved incident response
    - Exchange good practices
    - Exchange information

The Commission asks ENISA and Europol to:

- Establish digital forensic tools

Source: (Commission, 2009) & (Commission, 2013)

27 – Guitton's Findings

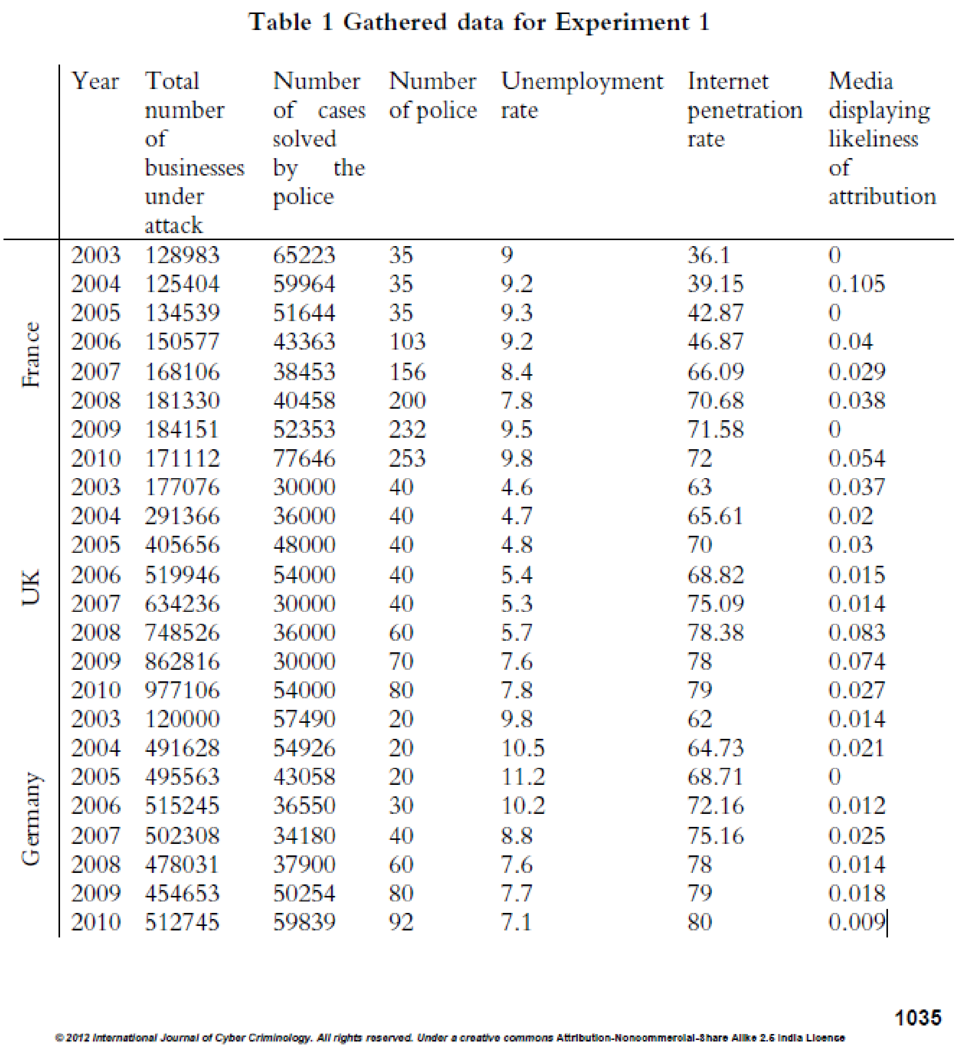


Table 1 Gathered data for Experiment 1

	Year	Total number of businesses under attack	Number of cases solved by the police	Number of police	Unemployment rate	Internet penetration rate	Media displaying likeliness of attribution
France	2003	128983	65223	35	9	36.1	0
	2004	125404	59964	35	9.2	39.15	0.105
	2005	134539	51644	35	9.3	42.87	0
	2006	150577	43363	103	9.2	46.87	0.04
	2007	168106	38453	156	8.4	66.09	0.029
	2008	181330	40458	200	7.8	70.68	0.038
	2009	184151	52353	232	9.5	71.58	0
	2010	171112	77646	253	9.8	72	0.054
UK	2003	177076	30000	40	4.6	63	0.037
	2004	291366	36000	40	4.7	65.61	0.02
	2005	405656	48000	40	4.8	70	0.03
	2006	519946	54000	40	5.4	68.82	0.015
	2007	634236	30000	40	5.3	75.09	0.014
	2008	748526	36000	60	5.7	78.38	0.083
	2009	862816	30000	70	7.6	78	0.074
	2010	977106	54000	80	7.8	79	0.027
Germany	2003	120000	57490	20	9.8	62	0.014
	2004	491628	54926	20	10.5	64.73	0.021
	2005	495563	43058	20	11.2	68.71	0
	2006	515245	36550	30	10.2	72.16	0.012
	2007	502308	34180	40	8.8	75.16	0.025
	2008	478031	37900	60	7.6	78	0.014
	2009	454653	50254	80	7.7	79	0.018
	2010	512745	59839	92	7.1	80	0.009

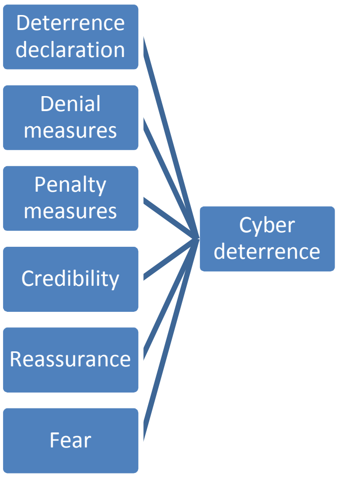
1035

© 2012 International Journal of Cyber Criminology. All rights reserved. Under a creative commons Attribution-Noncommercial-Share Alike 2.5 India Licence

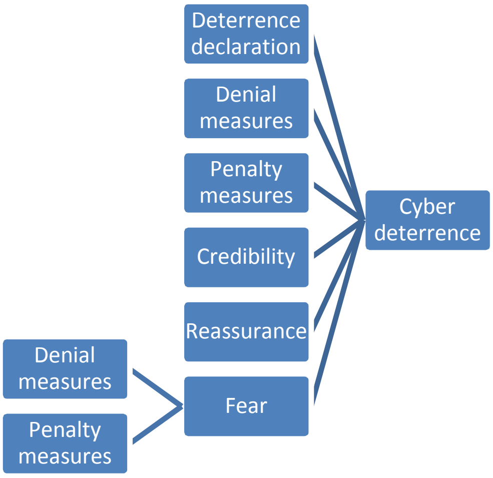
Source: (Guitton, 2012)

28 – Proposed conceptualisation of cyber deterrence

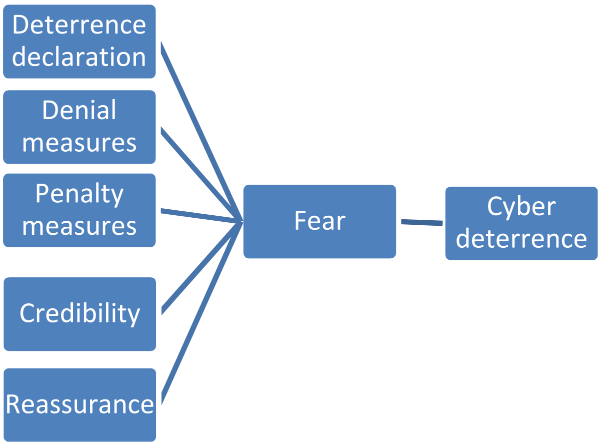
Currently these variables (exc. Cost-benefit calculation) measure cyber deterrence according to Goodman's conceptualisation:



However, each of these variables can be improved to enhance the ability to deter the enemy. To this end, Goodman argues that enhancing 'fear' can be done by enhancing denial and penalty measures (Goodman, 2010). Therefore:



However, a complication arises; the same variables are measures multiple times. As a result, the concept is biased towards the influence from denial and penalty measures. This thesis does belief that fear indeed is measured by, amongst others, denial and penalty measures, however this would require re-arranging the table to the following construct:



This thesis argues that the different elements highlighted by Goodman, actually measure the level of fear that they put into the eyes of a potential aggressor. To this end, it is the level of fear that these elements produce, which eventually result in the deterrence of an adversary. Nevertheless the framework, as conceptualised by Goodman, will be used in the remainder of the report; for methodological correctness.

29 – Kadi case law

For more information see:

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62005J0402:EN:HTML

For scholarly writings see e.g.:

Kokot, J. and Sobotta, C. (2012). *The Kadi Case – Constitutional Core Values and International Law – Finding the Balance.* The European Journal of International Law vol.23 no.4. Oxford University Press.

30 – summarizing table

Variable	**Indicator**	**Assessment**
Interest	*	*Very explicit*
Deterrence declaration	*	*CC** – very strong* *SSCA*** – strong*
Denial measures	Prevention	*CC – weak* *SSCA - strong*
	Futility	*CC – strong* *SSCA – strong*
Penalty measures	Retaliation	*CC – very weak* *SSCA - strong*
	Interdependency	*CC – weak* *SSCA – very strong*
	Counter productivity	*Unable to measure*
Credibility		CC – strong SSCA – very strong
Reassurance	*	CC – strong SSCA - strong
Fear	*	Unable to measure
Cost-benefit calculation	*	Unable to measure

* No indicator used

** Cybercrimes

** State-sponsored cyber-attacks

31 – Tax reduction on anti-virus programs

The key issue is preventing attacks rather than mitigation and recovering. To this end, the findings have shown that the EU still has limited capabilities to prevent attacks. For example DDoS attacks are performed by trained hackers that know what they are doing and require known and specific counter-measures to be taken. The EU can mitigate these attacks effectively (Schmidt, 2012). However, bot-net attacks contain groups of perhaps thousand or even hundreds of thousands computers which are infected by a virus. As a result, these computers can be remotely accesses and summoned to 'bombard' specific infrastructures with information requests, resulting in a shutdown of the website altogether. With the knowledge that world-wide there are millions of computers infected with viruses and malware and that these computers can be used as botnets, something needs to be done to protect the end-users. This will ultimately lead to the protection of the European interests since a large scale bot-net attack could potentially shut down CII's. The practical implication of this proposal is the reduction, or abolishment, of taxes related to anti-virus and malware software. Instead of spending tax money to establish institutions to mitigate an attack, the European MSs can miss out some small amount of tax income by making these types of software cheaper, ultimately protecting the source of potential attacks and themselves. By reducing the cost of these safety softwares, basic economic theories suggest that; more people will buy (better) anti-virus software. This in turn leads to more turnovers by the companies which should be made partners (second policy proposal) of the cyber-security network. These companies are now able to spend the extra income (without paying tax over it) on strengthening and improving anti-virus programs. A circle of protection is created and strengthened by introducing this proposal, or rather getting rid of superfluous government income.

32 – Cyber-transport

The cyber-infrastructure is very similar to public transport in the sense that packages can travel freely if the capacity allows them to. In the public-transport domain there are private companies dealing with these 'packages' (which are humans in this case), however they are under strict government control and have to oblige to strict regulations. In the cyber-infrastructure on the other hand these regulatory means have not entirely been imposed upon cyber-security companies. This thesis argues that if more and stricter regulations would be imposed upon the companies, a better protection can be guaranteed for citizens. Moreover, a closer cooperation between the businesses and other (supra) national institutions can be established.

33 – Europe should avoid 'securitisation'

The current European cyber-security framework has been criticized for creating securitisation. To counter the new threats in the cyber-domain Bendiek argues that the Commission and MSs tend to emphasize security over freedom, increasing security companies' and governments' power in this domain, whilst reducing the freedom to e.g. privacy (2012). This thesis argues that in the face of these new threats, Europe should not give in its ideological values. In his 'end of history' thesis Francis Fukuyama argued that the final form of governance is democracy and even though challenges and conflicts exist, this democratic form would survive and come on top (1992). Letting go of these democratic values effectively renders us the losers in history. Moreover, it would entail the loss of the governments' democratic legitimacy. This would increase the popularity and power within anti-government movements and eventually create a potential cyber-threat from within. Rather than choosing security over freedom, governments should tighten the strings around private security companies and improve the protection of citizens' data.