ifpol Institut für Politikwissenschaft	University of Twente The Netherlands
Westfälische Wilhelms-Universität Institut für Politikwissenschaft First Examiner: Prof. Reinhard Meyers	University of Twente School of Management and Governance Second Examiner: Dr. Rik de Ruiter

Governance and Cyberwar – The Role of the European Union

Julian Schibberges Heisstr. 28 48145 Münster Germany jschibberges@gmail.com	BA Public Administration (Special Emphasis: European Studies) Matikelnummer: 343921 Student ID: S0214515 Abgabedatum: 25.02.2011

Eidesstaatliche Erklärung

Declaration in lieu of oath

Ich versichere an Eides statt, dass ich die nachstehende Arbeit eigenständig und ohne fremde Hilfe angefertigt und mich anderer als der in der Arbeit angegebenen Hilfsmittel nicht bedient habe. Alle Stellen, die sinngemäß oder wörtlich aus Veröffentlichungen übernommen wurden, sind als solche kenntlich gemacht.

I declare in lieu of oath that I authored the following paper independently and without assistance and that I only used the resources indicated in the paper. All extracts that have been copied from publications analogously or literally are marked as such.

Julian Schibberges
Matrikelnummer: 343921
Student ID: S0214515
Münster, 16th of March 2011

____
Julian Schibberges

Abstract

The thesis investigates the relationship between cyberwar and governance using the examples of the European Union and NATO. Before addressing the two hypotheses, the main concepts of cyberwar and cyberdefense are defined and operationalized. The first hypothesis posits that the EU has already incorporated cyberdefense into its policy portfolio and tries to check this via the analytical framework of security governance. The second hypothesis takes a closer look at the principles of governance involved in cyberdefense and compares the European Union's multi-level governance with the intergovernmentalism of NATO. The assertion is that the EU is better suited to organize a European cyberdefense on account of its governance approach. Both hypothesis can be confirmed which leads to the overall conclusion that cyberdefense may be the policy field where the often called for common defense of the European Union could be realized.

Contents

Abbreviations

CCDCOE	= Cooperative Cyber Defence Centre of Excellence.
CDMA	= Cyber Defense Management Authority
CI	= Critical infrastructures
CII	= Critical Information Infrastructure
CIIP	= Critical Information Infrastructure Protection
CIP	= Critical Infrastructure Protection
CIWIN	= Critical Infrastructure Warning Information Network
DPPC	= Defence Policy and Planning Committee
EC	= European Commission
ECI	= European Critical Infrastructure
ENISA	= European Network and Information Security Agency
EPCIP	= European Programme for Critical Infrastructure Protection
ESDP	= European Security and Defence Policy
EU	= European Union
ICT	= Information and Communication Technologies
MLG	= Multi-Level Governance
NAC	= North Atlantic Council
NATO	= North Atlantic Treaty Organization
NC3A	= Consultation, Command and Control Agency
NCSA	= NATO Communication and Information Services Agency
WEU	= West European Union

1. Introduction

> A cyber society is a society where computerized information transfer and information processing is (near) ubiquitous and where the normal functioning of this society is severely degraded or altogether impossible if the computerized systems no longer function correctly. (Lorents, Ottis, & Rikk, 2009, p. 180)

No matter if one believes that the cyber society described above has already come true or is in line with the authors in thinking that it might still be a while, the information revolution has undoubtedly reshaped societies, economies and politics in the last decades. Information technology is a big part of the everyday live in the western world but also to a lesser extent all around the globe(Aronson, 2006, p. 624) and this begs the question what consequences this has. This thesis will focus on one of the less pleasant outcomes, namely the issue of cyberwar[1]. "Cyberwar is coming!" is the title of a 1993 study by the RAND Corporation and in retrospect this isn't so much a provocation as a mere statement of fact. Cyberwar as a form of warfare seems a very real phenomenon after the attacks on Estonia in 2007 and the surfacing of the Stuxnet-Computerworm in 2010. Undoubtedly there is still much debate about the concepts, occurrences and relevance of cyberwar but for the purposes of this thesis[2] cyberwar is considered possible and a legitimate threat. However this thesis will focus less on cyberwar but rather on "cyberdefense" and its consequences for European security. To that end two hypotheses are posited: First that that the European Union has already incorporated cyberdefense as a community concern and second that the European Union is better suited to organize a common cyberdefense than the other organization concerned with defense in Europe, NATO. Both hypotheses touch upon the larger discourse on the architecture of European security and the first one also upon defense integration in the European Union. The first hypothesis will use the analytical framework of security governance to determine if there is indeed a European dimension to cyberdefense while the latter will contrast the governing approaches of intergovernmentalism and multi-level governance and their "effectiveness" in addressing the challenges posed by this new form of warfare. Before the hypotheses will be explored however, a chapter will analyze the phenomenon of cyberwar and its related concepts in order to provide a deeper understanding of the issue and some useful ideas for operationalization. This approach to the topic will use a descriptive analysis of primary and secondary sources as well as of the relevant scientific literature to frame and answer the aforementioned premises. To answer the first hypothesis a concept of cyberdefense will be defined and

[1] In the literature it is written as both cyberwar and cyber war, it will be written as cyberwar here.
[2] Thesis will be referring to the paper at hand.

operationalized and then combined with the framework provided by security governance in order to analyze the structures, actors and policies that have been formed in the context of the European Union (EU) over the past years. To test the second hypothesis the concepts of multi-level governance and intergovernmentalism will be compared to see which governing mechanism better addresses the challenges posed by cyberwar, which have been defined in the first chapter. This test will be purely theoretical and not grounded in empirical evidence.

However it should also be pointed out that this view on the topic of cyberwar/defense will leave some aspects unexplored. This is not on account that they are not worthwhile subject for investigation or can't provide viable and interesting insights into the topic but rather on account of the limitations on the extent of this thesis. This includes but is not limited to the constructivist insight into the framing of threats (M. Dunn-Cavelty, 2008a) for instance or the issue of securitization of policy fields (Bendrath, Eriksson, & Giacomello, 2007). There are also some normative questions that will remain unanswered, such as the question who should provide security and the democratic legitimacy of that entity (M. Dunn-Cavelty & Suter, 2009, p. 184). For this thesis the notion that the state isn't the sole actor in the realm of security provision will just be accepted. Likewise the issue of domestic cyberdefense won't be further analyzed but just accepted as a variety of different approaches and policies (Abele-Wigert, 2006, p. 62; M. Dunn-Cavelty, 2005, p. 260; Enisa, 2011e).

2. Cyberwar in theory and practice

> "Obviously we can realize intuitively that cyberwar is warfare in cyberspace. However it is necessary to take into account that today's conception of cyberspace is constantly changing. "
> (Azarov & Dodonov, 2003, p. 3)

This chapter will focus on exploring the phenomenon of cyberwar by first elaborating on the history of the concept and then arriving at a useful definition. As the proceeding chapters will focus more on the issue of defense against cyber warfare, the subsequent part of this chapter will focus on how one can define and operationalize cyberdefense before looking at some of the events in the past decade that are considered as cyber warfare. These elaborations will serve as the basis for the later chapters and help to operationalize the concepts used.

Theoretical Framework

Before delving deep into the discussion of the European Union's approach to cyberwar, it is first necessary to adequately define the ideas and concepts behind the very terms cyberwar and cyberspace. This is underlined by the abovementioned quotation from a conference paper in 2003, in which the authors pointed out that the concept of cyberwar was still lacking a clear-cut definition(Azarov & Dodonov, 2003, p. 22). This next section will clarify the main terms and concepts behind the debate on cyberwar, such as cyberspace, netwar, information war, hyperwar, cyberattacks or cyberwar itself.

Cyberspace

The fundamental and main framework term obviously is cyberspace. The word cyberspace emanated not from the academic or military sphere but more or less from a science fiction novel by William Gibson called "Neuromancer": "Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding." (Gibson, 1984, p. 43). This, however, is more of a poetic understanding of cyberspace and has little use as an analytical concept. Ottis and Lorents point out a variety of different notions[3] and arrive at the following definition: "[C]yberspace is a time-dependent set of interconnected information systems and the human users that interact with these systems."(Ottis & Lorents, 2010, p. 268). This definition is useful as it captures not only the colloquial understanding of cyberspace[4] (e.g. the internet) but also the infrastructure behind the communication networks.

Cyberwar

With this definition in mind, it appears that cyberwar must somehow describe a form of conflict within cyberspace. However, as with the concept of cyberspace, the very definition of cyberwar has changed significantly over the years (and may even continue to change). To understand this development, one needs to look at several related concepts, most of which came up in the nineties. The first to be put forward was the term "hyperwar", phrased by E. Arnett in 1992. It was a terminology used to describe the very fast and automated way of fighting in the 1991 Iraq war through the extensive use of electronic and digital equipment (Arnett, 1992, p. 15). However, the "hyper"-part focused more on the notion of speed in modern-day combat and was not linked to the hypertext transfer protocol[5], as one might think. While the use of digital equipment did amount to the use of information systems in combat, combat was still fought in the traditional realms of land, air and sea. As such the information systems were used to enhance the conventional fighting capabilities and weren't used against each other via cyberspace. The term "cyberwar" was first used together with "netwar" in a 1993 publication by the RAND Corporation titled "Cyberwar is coming!"(Arquilla & Ronfeldt, 1993). While the notion of netwar, like hyperwar, sounds related to

[3] See (Ottis & Lorents, 2010) and(Strate, 1999) for more details.
[4] Synonym expressions used in this thesis will be digital realm
[5] See http://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol

cyberspace, this linkage is deluding as netwar refers to an engagement between nations or societies where each side tries to "to disrupt, damage, or modify what a target population "knows" or thinks it knows about itself and the world around it (Arquilla & Ronfeldt, 1993, p. 28)" and thus provides little insight. It has little to do with conventional warfare and has also little focus on warfare in cyberspace. Cyberwar, as used by Arquilla and Ronfeldt, had also very little to do with cyberspace but was more of a concept for all military operations carried out by means of information-related principles (Arquilla & Ronfeldt, 1993, p. 30). Its goals were to "...disrupt [...] if not destroy [...] the information and communications systems, broadly defined to include even military culture, on which an adversary relies in order to "know" itself...". Considering their broad outlook it is no wonder they believed that Mongols were the first to wage cyberwar (p. 43). Indeed their idea of cyberwar may be more related to another concept called "information war". The idea of information war was first put forward by Thomas Rona (Rona, 1976) but was substantially modified and further specified by M. Libicki (Libicki, 1995, p. 4). Libicki defined information warfare as the gathering, denial and manipulation of information (Libicki, 1995, p. 8) and identified seven forms of it (Libicki, 1995, p. 7). Hacker warfare and cyber warfare are two of these forms but they are seen as only a small part of the larger idea of information warfare. Indeed, he compares the notion of cyberwar akin to the notion of air combat in Victorian times(Libicki, 1995, p. 75). This may be partially explained by the fact that he considers, what he terms simula- and Gibson-warfare (Libicki, 1995, pp. 79-81), as part of it. However, there is already a more current notion present as one can see in the concepts of hacker warfare (Libicki, 1995, p. 49) and semantic attacks (Libicki, 1995, p. 77) though he disregards both as significant threats. While this work provides a context for cyberwar it doesn't provide an adequate definition. Especially the differentiation between hacker warfare and cyberwarfare limits the range of the concept while the inclusion of the very futuristic concepts of simula- and Gibson-warfare extends it too far for the purposes of this thesis. Another point that is worth mentioning is his idea that information operations and therefore also cyberwar can't be seen as a separate discipline of warfare(Libicki, 1995, p. 97) which is interesting considering the remarks of General Fogleman in the same year, calling information war the "fifth dimension"[6] of warfare(Fogleman, 1995)[7].

Looking a few years ahead, a slightly different approach to cyberwar can be seen as evident in an article of the Winter Issue of NATO Review in 2001. Cyberwar, nowadays, appears to be a lot more focused on what Libicki would describe as semantic attacks and hacker warfare and a differentiation has been devised, distinguishing several levels of severity (Shimeall, Williams, & Dunlevy, 2001, p. 17). The authors differentiate between cyberwar accompanying "regular" military operations, restricted cyberwar and unlimited cyberwar. The delineation is done by the attacker's choice of

[6] Land, Sea, Air and Space being number one through four.

[7] This is also the stance of the U.S. Air Force: http://www.airforce.com/learn-about/our-mission/

target: Military information systems when it comes to military operations, communication systems in limited cyberwar to deny the enemy information but without causing physical harm and in an unrestricted cyberwar there would be no differentiation between civilian and military targets and the attacks would cause physical and human damage. This would be done by targeting the national critical infrastructure without differentiating between government and private property (Shimeall, et al., 2001, p. 17). This last notion is very central to our current understanding of cyberwar, where critical infrastructure (CI) and especially critical information infrastructure (CII) play a central role. The endgame for unrestricted warfare would be a nation devastated by human loss and a broken society and economy (Shimeall, et al., 2001, p. 17). The article also mentions very specific concepts of "cyberattacks" such as Distributed-Denial-of-Service-Attacks (DDOS)[8] and malicious software codes. This idea about cyberwar already comes fairly close to the current understanding. Especially the separation of cyberwar and cyberattacks is useful. Saalbach defined cyberattacks based on the work of Wilson (2007, p. 3) as "attack[s] on computers and their data, the computer network and the systems dependent on the computers."(Saalbach, 2011, p. 4). If one considers computers as information systems this is very compatible with the adopted definition of cyberspace. However a cyberattack doesn't necessarily constitute a cyberwar, as it could describe any kind of malicious activity on the internet. Indeed, this is a discussion that has been prominent in many recent publications, where the question of attribution as well as the characterization of cyberattacks as an act of war is discussed. The problem with cyberattacks is that the perpetrator can remain hidden thus making deterrence very difficult. Also, cyberattacks on valuable targets such as CI are usually not adhoc-operations but must be planned more strategically. This begs the question, however, if the simple penetration of a system and the possible placement of malicious software is an act of war or only its execution. Yet, the debate is too extensive and complex to be reproduced here with substance[9]. Should a cyberattack not be the same as a cyberwar though one needs to define the threshold (Lewis, 2009, p. 3). Myriam Dunn-Cavelty provides us with a useful analytical framework for making this distinction (Myriam Dunn-Cavelty, 2010, p. 1). She creates a "cyberladder"[10] where different cyberattacks are grouped by their potential damage and intent. This is useful for delineating cyberwar from other malicious internet activity. One can see that cybervandalism and internet crime (what Libicki probably understood as hacker warfare (Libicki, 1995, p. 49)) are on the bottom as they concern mostly individual citizens or companies. Cyber espionage in this context is also defined mainly as corporate espionage. Cyber terrorism concerns cyber attacks that cause loss of life and

[8] If you imagine a computer/information system as a call center, a denial-of-service-attack would be someone calling all the time to block capacities. A distributed attack would be thousands of people calling thus preventing the call center from operating. A real DDOS uses bits and bytes but similarly prevents a server from answering legitimate data requests. For more read (Zuckerman, Roberts, McGrady, York, & Palfrey, 2010, p. 15)

[9] See for example (Libicki, 2009) or(Reich, Weinstein, Wild, & Cabanlong, 2010)

[10] See Annex, Picture 1

property with the intent of intimidation but as the author points out(Myriam Dunn-Cavelty, 2010, p. 2) and others concur(Hunker, 2010, p. 5), so far none have been carried out and that they are unlikely to happen. The last rung then is cyberwar, which is only very broadly defined at this stage. As above, it is seen as part of the concept of information war and adjunct to other more traditional types of warfare (Myriam Dunn-Cavelty, 2010, p. 2). There is however no differentiation for her between cyberwar and cyber state espionage, which is justifiable because the threshold is blurry in theory and in practice[11]. Yet comparing it to the "analog" counterparts, it is apparent that state espionage is more or less continually carried out and to a greater or lesser extent tolerated (Lewis, 2009, p. 2) unlike acts of war would be. Therefore it would be proposed to use the definition already put forward by Shimeall for unlimited cyberwar (Shimeall, et al., 2001, p. 2) as the targeting of critical infrastructure and exclude cyber espionage on practical grounds(Sommer & Brown, 2011, p. 81). This is insofar justified as critical infrastructure protection (CIP) is seen as the defense component to cyberwar by many authors (Cornish, Livingstone, Clemente, & Yorke, 2010, p. 22; Myriam Dunn-Cavelty, 2010, p. 3; Saalbach, 2011, p. 10) and would also fit with a framework for cyberconflict devised by Lewis(2009, p. 6). With this at hand, cyberwar for the purposes of this thesis can be defined as cyberattacks within and through cyberspace against the critical infrastructure of a state[12]. To be able to use the concept though, there is the need to define what critical infrastructures are and to conceptualize how their protection can be realized.

Critical Infrastructures and their Protection

Critical infrastructures as a term doesn't stem from the cyberwar debate but dates back to the idea of system vulnerability(Collier & Lakoff, 2008, p. 18) which came up around World War I and the advent of air power(Collier & Lakoff, 2008, p. 20). The central idea is that wars are no longer fought between armies but between nations as a whole hence blurring the distinction between the civilian and the military sphere(Collier & Lakoff, 2008, p. 20). This lead to a thinking were the aim of war wasn't anymore to defeat the enemy army but to defeat the nation as a whole with the consequence that viable centers of economic and social life became legitimate targets. An example of a war fought along this maxim could be the US air campaign against the German industrial sector in World War II(Collier & Lakoff, 2008, p. 21). But at the same time system vulnerabilities became interesting for offensive military action, military planners also had to devote some thought on protecting those "systems" that were important for the functioning of their own society. The whole idea flourished in the Cold War and was reinterpreted under a national security paradigm in the 1970's(Collier & Lakoff, 2008, p. 31) but had only small relevance in comparison to concepts such as deterrence(M. Dunn-Cavelty, 2008b, p. 40). Nonetheless the national security approach defined the framing of the

[11] If one hacks a computer one can both steal information as well as manipulate it.

[12] Or any other organization as long as it's CI is defined.

issue from then on. In the 1990's the issue was revitalized under the name of Critical Infrastructure Protection mainly due to the influence of the information revolution, as Dunn-Cavelty claims(M. Dunn-Cavelty, 2008b, p. 40).

The exact definition what constitutes critical infrastructure depends very much from country to country but the most commonly named infrastructures are the banking and financial sector, government (democratic institutions, services, security forces), telecommunication and information and communication technologies, emergency and rescue services, energy and electricity, the health sector, transportation, logistics and distribution and water supply(M. Dunn-Cavelty & Kristensen, 2008, pp. 1-2; Saalbach, 2011, p. 4). In sum, CI are those infrastructures without which society and economy would break down. With the advent of the information revolution many of these infrastructures have undergone a major change in the way they are operated. Obviously this didn't happen equally and at the same pace(M. Dunn-Cavelty & Brunner, 2007, p. 5), for the military for instance the so called "revolution in military affairs" started already in the 1980s (Metz & Kievit, 1995, p. 1), but by today nearly every aspect of our lives is affected by Information and Communication Technologies (ICT). While for most people this is most noticeable in their private lives, this is also very true for modern industry and infrastructure. Today most machinery is no longer controlled by electrical buttons and switches but via digital controllers being operated from computers(Saalbach, 2011, p. 3). This however lead to some concern which was most publicly voiced in the Presidential Commission on Critical Infrastructure Protection in 1997(M. Dunn-Cavelty & Kristensen, 2008, p. 2). The critical information infrastructure (CII) that was by then the backbone of the CI(M. Dunn-Cavelty & Brunner, 2007, p. 11) did not only fuel innovation and progress but also became it's the Achilles heel(M. Dunn-Cavelty & Brunner, 2007, p. 7)[13]. This is very apparent in another aspect of CI/CII, which is the interconnectedness of today's infrastructures. It is true all around the globe but especially in Europe with the EU being a major force of integration. Not only are economies and in particular the financial sectors intertwined but also the European information infrastructure. Looking at a map of the deep-sea cables[14], the backbone of the internet, one can see that many of them arrive in the UK or the Netherlands. Should any of those two countries somehow lose their connection it would affect data transfers across the continent. Likewise countries in Central and Eastern Europe depend on their neighbor's networks for their internet access. This internet access is crucially important for business in times of cloud computing[15] but also many normal business transactions depend on functioning networks. However internet infrastructure is not the

[13] This shows a small problem of definition, as theoretically there is a difference between CI and CII and both also encompass more than just the digital aspect of infrastructure. Thus for the purposes of this thesis, when referring to either, only the digital aspects are meant. To denote that both kind of infrastructures are meant they will usually be referred to as CI/CII or CIP/CIIP.

[14] See Annex, Picture 2

[15] Renting software and computing time over the internet rather than buying and maintaining it locally.

only infrastructure that is interconnected. The energy network is another example and one that also depends highly on software. Energy shortages in Germany can be somewhat mitigated by buying electricity from surrounding countries but simultaneous failures in several countries might be hard to compensate (though the effect might also not be as big as expected(Hunker, 2010, p. 5)). Pipelines for gas and oil are also running across the continent as is the transportation infrastructure such as trains. Both also rely on information systems to function properly. The point of all this is, that CIP in the European context is not limited to the respective nation state. Cable failures in Amsterdam or a malfunctioning pipeline in Germany will have transboundary effects.

Critical Infrastructure Protection

The question, how to protect against the danger from CI failure, be it because of nature, terrorism or war, became therefore more urgent. Against the conventional forms of warfare the armed forces of a nation were able to provide protection but what about the threats from cyberspace? A key difference however to the traditional spheres of warfare is the question of ownership and the ability to protect. Especially after the eighties and nineties many infrastructures that were previously run by the state were privatized(M. Dunn-Cavelty & Suter, 2009, p. 179) and with that step the security of that infrastructure was no longer controlled by the state. Unlike the physical buildings the ICT-Systems can't be protected by building a bunker or stationing and anti-aircraft-canon next to it. As long as a government doesn't want to take continuous responsibility for the ICT-Security (and even then it would be questionable if any corporation would like such close scrutiny on its business) it is unable to protect a particular asset against cyberattacks(M. Dunn-Cavelty & Suter, 2009, p. 179). Obviously it would be able to regulate security standards via law but controlling the implementation would be difficult(M. Dunn-Cavelty & Suter, 2009, p. 183). So in essence, while the conducting of cyberwar is a matter of the military, much of the protection against it lies in the hands of the private sector(Myriam Dunn-Cavelty, 2010, p. 3). There have been several ideas how to organize CIP among them Public-Private-Partnerships, Network Governance and Collaborative Governance, though each has to address several problems. The overarching concern is the fact that that the interests of governments and the private sector hardly converge as the one party sees the issue as a matter of national security while the other views as a matter of business continuity(M. Dunn-Cavelty & Suter, 2009, p. 181). For a business, security measures are first and foremost costs(Donahue & Zeckhauser, 2006, p. 445). Costs that may be necessary to ensure the businesses' viability but that are not that much concerned with providing nation-wide security. The government on the other side is concerned with the security of its society but, as pointed out before, has little control over the implementation of security measures. At the same time the private sector may have limited information at its disposal, hampering its own efforts to protect the infrastructure(M. Dunn-Cavelty & Suter, 2009, p. 181). An additional point is, that private sector cooperation in the process of setting, implementing and verification of standards, regulation and information sharing practices can be crucial as private actors have a better understanding of their business sector and may be less easily tricked (M. Dunn-Cavelty & Suter, 2009, p. 183) The traditional idea would be a Public-Private-Partnership(M. Dunn-Cavelty & Suter, 2009, p. 180) where the both concerned parties come together to tackle this joint (albeit differently viewed) problem. However Dunn-Cavelty and Suter point out that while this approach has been more or less practiced, it is less than ideal (2009, p. 181). Instead they propose a form of network governance or meta-governance, where the government primarily acts as an organizer of networks that fulfill certain goals(M. Dunn-Cavelty & Suter, 2009, p. 183). The government determines these goals and then verifies if they are met. However it relies on peer-review to evaluate the measures taken by the individual businesses. Collaborative governance[16] basically stipulates that the government gives certain benefits to private businesses in return for enhanced security(Donahue & Zeckhauser, 2006, p. 450). The mechanisms behind it are the different forms of discretion a government allows private entities to fulfill a government set goal or task(Donahue & Zeckhauser, 2006, pp. 439-445).

Besides the governing concept by which CIP/CIIP is organized there is also the question what to do to enhance CIP/CIIP. Dunn-Cavelty points out that this as much a question of perception as of measures (2005, p. 260). The approach taken by the concerned entity can see CIP/CIIP as an issue of national security, of economics or of law enforcement(M. Dunn-Cavelty, 2005, p. 261). Despite the outlook on the problem, there are several measures that are mainly used to enhance CIP/CIIP(Esterle, Ranck, & Schmitt, 2005, p. 32). The main measure to enhance protection is information sharing(M. Dunn-Cavelty & Suter, 2009, pp. 180-181)[17] such as exchanging best practices, information about potential security threats or security incidents and about technological developments(Esterle, et al., 2005, p. 32). Another and more traditional way is the setting of standards (Donahue & Zeckhauser, 2006, p. 450; M. Dunn-Cavelty & Suter, 2009, p. 183) for security or service availability. Lastly there is the forming of Computer Emergency Response Teams (CERT) (Enisa, 2011a) as a manner to respond to the potential cyberattacks, and their cooperation/coordination. All these measures will prove futile however, if there is no incorporation of the private sector. As already pointed out the private sector has a very central role and can be vital in the setting, implementation and verification of policy(M. Dunn-Cavelty & Suter, 2009, p. 183).

Synopsis

To sum up, the target of any potential cyberwar is the CI or CII of an entity. They are understood as the infrastructure that is critical to the functioning and well-being of a society and an economy.

[16] See (Donahue & Zeckhauser, 2008) for more details.

[17] Their critique is valid but for the purposes operationalization it is more important to list the potential forms of cooperation than the optimal ones.

Protecting this infrastructure is difficult for a government because most of it is privately owned and private actors often don't have the necessary resources and information at their disposal. While security is a common concern for both parties, their view on it is very different. To enhance CIP/CIIP a government needs to engage the private actors through a variety of means. While regulation is the most obvious choice, many governments opt for PPP or some form of network/collaborative governance to incorporate the private sector in the governance of CIP/CIIP.

Bringing in the Practice

So far, the considerations of cyberwar have been rather theoretical in nature and the question arises how far cyberwar can actually be considered a real phenomenon. Saalbach devotes part of his 2011 paper to a recapitulation of events that he considers instances of cyberwar (Saalbach, 2011, p. 12). The following section will take a look at these events and evaluate against them the preceding definitions. However, the word of caution by Saalbach should be repeated: The recounts of the events are usually the stories of only one of the allegedly involved sides.

These examples can be broadly placed into four categories: Vandalism, Espionage, Cyberwar and "Maybes". Examples for vandalism would for instance be the defacement of websites during the Kosovo War or the Georgia War. While the websites may belong to government entities, their function is not one of critical infrastructure (Shimeall, et al., 2001, p. 17) and therefore mainly psychological. The attacks on western government computers in 2007/2008 as well as the attacks dubbed "Moonlight Maze" should be considered instances of espionage as the main function seemed to have been the copying of data and not the destruction or manipulation of CI/CII. The maybe category, for instance, comprises what some consider the first example of cyberwarfare, the 1988 Russian pipeline explosion. This was said to be the work of a "logic bomb", malicious software code smuggled into Industry-Control-Software (ICS) by the USA that was later stolen by Russia. Considering our definition of cyberwar this wouldn't really fit and would seem more like "cybersabotage". The "Hainan" attacks may be acts of cyberwar but it seems that they targeted personal computers and not so much the larger CII. However, if some of these computers were used to run CI/CII then this would be an example. The shutdown of communication networks in Serbia during the Kosovo War could be an act of cyberwar but no information is given on the means.

What can be called cyberwars or acts of cyberwar, in line with our definition, are the instances of Estonia in 2007, Georgia in 2008 and the Stuxnet worm in 2009/2010. The attacks on Estonia started in April 2007 and lasted for nearly 22 days. It was mostly DDoS-attacks that targeted websites and email services but also bank and DNS[18] servers. While this might not seem as critical for the average European, one has to keep in mind that Estonia is a very "digitized" society (Lorents, et al., 2009, p.

[18] Domain Name Server, basically an address book that translates an address like www.utwente.nl to its numeric equivalent.

182). Many government and financial services can be mainly obtained online and the unavailability of a bank server can cause serious economic damage. Likewise, an attack on the DNS server prevents Estonians from ever reaching any websites effectively cutting them off the internet. Luckily these attacks didn't cause physical harm but they prevented the Estonian society from business-as-usual for weeks(Lorents, et al., 2009, p. 184). The cause for the attacks is supposed to be the removal of a Statue of a Soviet soldier and therefore the attacks are attributed to Russia or Russian groups, however this could never be proven(Ottis, 2008, pp. 1, 6). Russia was also considered the perpetrator of the cyberwar launched against Georgia in 2008, though considering the ensuing real war the odds are indeed very high. Like in Estonia the cyberattacks were also carried out via DDoS and targeted many government and media websites but also the banking and transportation infrastructure (Saalbach, 2011, p. 14). There are on the other hand claims that it all was mere cybervandalism (Cyberwarfare: Marching off to cyberwar, 2008). Nonetheless there definitely were attacks and they were partially targeted at CI/CII which is why according to the definition adopted this would constitute cyberwar. This case in addition is interesting because it was the first instance of cyberattacks being used in conjunction with physical attacks (though Russia didn't take responsibility for the cyberattacks), showing the potential, though in this case underutilized, use of cyberwarfare. The last instance considered is the case of Stuxnet. Stuxnet[19] was a computer worm discovered in 2009 that spread around the world and was at first considered fairly harmless, as it didn't do any obvious damage (The Economist, 2010b). After some time however it was discovered that the virus looked for a special ICS-Software by Siemens and manipulated it while simulating a completely normal course of events for the user (a semantic attack). After further deciphering it was learned that the virus would only "attack" if a certain setup was found which many people thought resembled the Iranian nuclear enrichment facilities (The Economist, 2010b). While it could not be proven, it was widely speculated that this virus was used to destroy a large number of Iranian centrifuges, therefore setting their nuclear program back for years (The Economist, 2010c). The alarming nature of this virus was that it manipulated ICS in a way previously not thought possible which is cause for grave concern as such ICS are present in most modern infrastructure systems (The Economist, 2010a). While it might not be easy to recode this virus to attack other kinds of infrastructures, with the right resources, such as knowledge and money, it is definitely possible. With software like that some of the Armageddon scenarios are not as farfetched as previously thought (though still highly unlikely). In some way, malicious software can replace a strategic bomber force today. A point also worth noting is that the attack couldn't be contained to the supposed target and that infection was widespread (though rather harmless). It shows that the interconnectedness of the

[19] For an extensive analysis see http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

world makes using cyberattacks risky as the intended target may not always be the sole entity affected.

Synopsis

First and foremost, it can be concluded that cyberwars are no farfetched scenarios(Eriksson & Giacomello, 2007, p. 174) from the distant future but that they are a very real threat today. The horror scenarios that some scholars and many newspapers imagine might be wrong, but especially Stuxnet has shown, that cyberattacks have a serious potential for damage to human life and property. Today cyberwar is just another dimension of warfare and can be used in conjunction to but also independently from regular warfare. Nonetheless, it holds true that "serious cyber attack independent of some larger conflict is unlikely." (Lewis, 2009, p. 7), but this conflict must not be military. Secondly, while the asymmetric nature of cyberwars is always underlined, those examples that are known show that it might be the other way around: Powerful states using cyberattacks to punish or as a means to achieve goals that otherwise could only be achieved through blunt force. Especially, the "invisibility" factor is very important as so far no country has ever claimed responsibility for any attack. This is another point where the discussion in the early 2000s went wrong: The threat from terrorist or single groups is fairly low. Most examples cited above needed the resources of states behind them to succeed. This is not surprising, considering that attacks on infrastructure don't only require the knowledge of the information systems but also of the infrastructure itself. This is something most hacker groups, however adept they may be at breaking into computers, just don't have. It must be either expensively bought or developed which is something most non-state actors just don't have the resources to. The key differences to other forms of warfare are threefold. First the targets of cyber warfare and their protection are mainly in the hands of private companies with limited potential of direct state involvement. Second, in today's world these infrastructures are highly interconnected and may have relevance beyond the nation state they are situated in. Likewise attacks may have effects beyond their intended target. Third, the clandestine nature of cyberwar prevents deterrence from being effective and may provide little warning in advance of an attack. Thus the efforts to protect CI/CII need to be constant as there may be no time to build up defenses.

Conclusion

What are the conclusions to take from this chapter? For once, one needs to recognize that cyberwar is not a fantasy but a very real aspect of modern-day warfare. While cyberattacks vandalizing websites are the most obvious, the true cyberwar targets infrastructure that is critical to the functioning of a state. In this sense it can function very similar to a strategic bomber force and can provide even governments of states not in the G8 with greatly enhanced military capabilities. That impact can be achieved has been shown by the attacks in Estonia and the Stuxnet-worm, however these attacks so far have been of limited character and it remains to be seen if cyberwar can be waged with a more general scope. As a consequence the central aspect for a state or a community of states preparing for this new kind of conflict is to enhance the CIP/CIIP of their nation. As outlined above there are several measures and approaches how to do so. The However, taking into consideration the decentralized nature of cyberspace and the interconnected infrastructure of today, focusing solemnly on a domestic approach might be falling short. A deep-sea cable that is knocked out in the Netherlands will have repercussions for the speed and quality of service in central Europe as would an attack on French banking servers. This leads to the conclusion that CIP/CIIP is more effective on a regional or international level.

3. A European Union Cyber Defense?

After we have examined the concepts and reality of cyberwar and cyberdefense in the last chapter, this chapter will turn to the issue of a European Union (EU) cyberdefense. This is an interesting issue because it taps into the general debate about defense/security integration in the European Union which for a long time had been a very contentious topic. While a common defense has been the goal since the treaty of Amsterdam, this hasn't lead to substantive integration in that policy field. With the ratification of the Lisbon treaty things have progressed and the EU cooperates when it comes to out-of-area-missions, the defense of Europe is still in the domain of NATO. So the first thesis, that the European Union has already incorporated cyberdefense into its portfolio has implications for its identity as a security actor. Considering cyberwar as a military discipline and therefore the defense against it as a matter of domestic external security, then the integration of cyberdefense in the EU marks also a step further to becoming a comprehensive security actor. In order to determine this, the question if the EU has already incorporated cyberdefense into its policy portfolio has to be answered. In order to provide a more thorough answer, the question will be rephrased to "Is there a European dimension to the security governance of cyberdefense." In order to provide an answer, this chapter will look at the theoretical frameworks of European integration, on the development of European security and defense policy in general and then in particular when it comes to cyberdefense ergo CIP/CIIP. These developments will be analyzed via the framework of security governance that will be devised.

Theoretical Framework

Before taking a look at the specific EU measures and institutions concerning cyberdefense there is the need to introduce some theories and concepts that will be used for analysis in this and the next chapter. These are the integration theories of neo-functionalism and intergovernmentalism and the concept of Multi-Level Governance (MLG). While these are not all that are potentially relevant, the choice was limited to them as they provide the greatest utility for the inquiry at hand. The theory of intergovernmentalism is one of the central theories why and how supranational integration takes play but it describes the modus operandi for many international organizations such as for instance NATO. MLG is the currently most used concept to analyze the EU but its status as a theory is debated. However the argument is made by George that actually MLG picks up many of the assumptions and predictions made by neo-functionalism, which is the reason why this theory is also explained here. There are obviously more theories that can be applied to the study of EU integration such as constructivism or neo-liberal institutionalism. While they are generally valuable tools to explore the complex of cyberwar(M. Dunn-Cavelty, 2008a), they yield little additional insight to this inquiry and are therefore being disregarded.

Neo-functionalism

Neo-Functionalism was the first theory that tried to explain the integration processes of the European Union or, as it was introduced in the 1950s, the European Communities(Stroby Jensen, 2009, p. 72). There are three ways this theory accounts for policy integration, spillover, elite socialization and supranational interest groups. The spillover thesis proclaims that cooperation in one policy area would lead to cooperation in adjacent policy areas(Stroby Jensen, 2009, p. 73). This is because for cooperation to function in one area there is the need to regulate related policy fields as for example the creation of the single market lead to cooperation in safety standards(Stroby Jensen, 2009, p. 76) as it was required to make the single market work. This thesis can be broken down further into three different types of spillover, functional/technical, political and cultivated. Functional or technical spillover is pretty much explained by the previous example, spillover because of functional forces. This is contrasted by political spillover where political elites focus more on European solutions than national ones and cultivated spillover, where integration is fostered by supranational organizations(Stroby Jensen, 2009, p. 76). The elite socialization thesis states that those involved in integration/cooperation processes will develop supranational loyalties and preferences that subsequently lead to an increased cooperation(Stroby Jensen, 2009, p. 77). The supranational interest group thesis work fairly similar in the sense that interest groups develop a supranational focus when they realize the potential of influence they may have at supranational level and thus lobby their national governments for more integration(Stroby Jensen, 2009, p. 78).

The critique of neo-functionalism is twofold: There are theoretical objections that claim that supranational entities as well as the elite socialization have been erroneously conceptualized and that supranational organizations are mere “appendages” of intergovernmental conferences (Stroby Jensen, 2009, p. 80). Empirically the absence of integration in the seventies and early eighties has been declared incompatible with neo-functionalism (Stroby Jensen, 2009, p. 78).

Intergovernmentalism

The theory of intergovernmentalism takes a very different approach to integration. Being based in the theory of neo-realism, intergovernmentalism sees the states as central actors in the international sphere and doesn't recognize the EU as a force of its own but rather a form of interstate cooperation. There is no transfer of sovereignty to the EU, but as Cini puts it, only "sharing" or "pooling"(Cini, 2009, p. 89). A development of classical intergovernmentalism is the notion of liberal intergovernmentalism put forward by Andrew Moravcsik (Cini, 2009, p. 96). This theory takes a supply and demand approach to the issue of European integration where demand is created by the national governments and supply is produced by intergovernmental negotiations (Cini, 2009, p. 97). Governmental demands for integration are shaped by the domestic sphere e.g. influenced by the different actors from civil society and the private and public sector. International negotiations then determine the policy as well as the institutional form of the solution through bargaining. In this stage states are considered to be unitary actors and the only ones that matter (Cini, 2009; Jachtenfuchs, 2005, p. 401). International institutions serve as facilitators of inter-state bargaining and also as means to ensure compliance (Baylis, 2006, p. 304; Cini, 2009, p. 98).

The critic of intergovernmentalism as wells as liberal intergovernmentalism is mainly empirical, i.e. that states are not unitary actors and that subnational as well as supranational do have influence on positions as well as negotiations (Cini, 2009, p. 99; Jachtenfuchs, 2005, p. 401).Critic specifically for liberal intergovernmentalism is its narrow conception of the state and allegation that as a theory it can't be disproven (Cini, 2009, p. 102).

Governance

Governance is the separation of government and governing, where the government isn't the only actor that is involved in the management and regulation of society (Dunn-Cavelty & Suter, 2009, p. 182). The concept was developed in the late seventies/ early eighties in the context of government reforms in the USA and the UK. As such it is inherently connected to the ideology of neoliberalism. The idea behind it is the separation between governing and government and the expansion of the potentially governing actors. This was related to the neoliberal reform programs of that time insofar as the idea was to increase the outsourcing of government services/functions via market system (Bevir & Rhodes, 2001, p. 3). However apart from the ideologically influenced neoliberal governance theory there also the network governance approach that takes into account the neoliberal public sector reforms but sees the effects not as intended by neoliberal theory but as a fragmentation of government resulting in a network structure of governance instead of a market system(Bevir & Rhodes, 2001, p. 6). Thus management and regulation of issues are not done by a central authority anymore but by "self-organizing, inter-organizational networks" (Bevir & Rhodes, 2001, p. 18). A further differentiation can be made between a centered and decentered approach to governance

(Bevir & Rhodes, 2001, p. 19) with the former using a more positivistic and the latter a constructivist approach.

Multi-Level Governance

The idea of governance has been applied to the study of the European Union and has been refined in the concept of Multi-Level Governance (MLG). As a theory it moves away from the state-centrist approaches of intergovernmentalism and puts is focus on the EU as a source of policy output. It still sees the states or rather the state executives as central actors but it doesn't limit the political power to only them(Marks, Hooghe, & Blank, 1996, p. 346). Instead it proposes a model where policy is made by a number of actors on supranational, national and subnational levels. They are independently interconnected within and across levels. There is debate in how far MLG can be classified as a theory or if it is rather an analytical framework(Jordan, 2001, p. 201; Rosamond, 2009, p. 116). The argument in favor is made by actually linking it to Neo-Functionalism and treating it as an reformulation of that theory(George, 2005, p. 112). Insofar MLG draws from the ideas neo-functionalism as well as from governance. In any way, for the purposes of this thesis the ability of multi-level governance to serve as an analytical framework is more important than as an explanatory theory of European integration.

Security Governance

While MLG provides the greater context for the European Union, the specific concept of interest is that of security governance. The use of the concept of meta-governance devised by Dunn-Cavelty and Suter was considered but ultimately decided against because it provides a rather specific concept how to (re-)organize CIP governance and wouldn't have proved very useful in analyzing what is actually already present(2009, p. 183). Nonetheless, it is compatible as a concept with security governance. To be able to use the governance approach to determine if there is a regulatory capability when it comes to the issue of cyberdefense there is the need to define the analytical framework to evaluate the EU activities against. The basis for defining security governance is found in a text from 2004 by Mark Webber et al. who give the following definition:

> European security[...] governance involves the coordinated management and regulation of issues by multiple and separate authorities, the interventions of both public and private actors (depending upon the issue), formal and informal arrangements, in turn structured by discourse and norms, and purposefully directed toward particular policy outcomes. (Webber, Croft, Howorth, Terriff, & Krahmann, 2004, p. 4)

This definition is later clarified to have five components(Webber, et al., 2004, p. 8) which are worth taking a closer look. The heterarchical[20] relationship between the actors is a key notion of governance theory, however empirically it is evident that the state is still the primary actor(Webber, et al., 2004, p. 6). Nonetheless this is in line with the concept of multi-level governance as the actors on the different levels are not constrained by interacting through the next higher level (hierarchy) but are free to interact with any actor on any level. Thus to be able to speak of heterarchical structure of actors in a European context one would need to see supranational, national and subnational actors that interact freely (without the constraints of a hierarchy) with each other. This interaction according to Webber et al. should be by a large number of actors that come from the public as well as from the private sector(p. 8). While one could debate what a "large" would mean in this context, for the purposes of this paper this will be more than 29 actors, the number being chosen as to incorporate all member states as well as a representative from the commission and the parliament. Formal and informal institutionalization would imply that there should be arrangements on a European level that reflect either approach. The formal arrangement can identified as the codified decision and consultation mechanisms. As for the informal arrangements, since the codification of the open method of coordination (OMC) in 2003, there are the policy networks that are a form of informal consultation/coordination mechanism(Coen & Thatcher, 2008, p. 54). Thus if there is the presence of formal European regulation/coordination and informal modes of regulation/coordination in a certain policy field this requirement would be met. The point that relations between the actors should be ideational and structured by norms and discourse is difficult to operationalize for any special field of European politics. The European Union itself is a manifestation of an ideational relationship between its members and as an institution is governed by certain norms such as democracy or subsidiarity. Likewise it is shaped by the respective treaties which are a form of discourse. This is also echoed in Webber et al. (2004, p. 17).Therefore this feature can be generally affirmed for the European Union and maybe reaffirmed by specific features of the policy field in question. Lastly the common purpose can be viewed in structural and process terms (Webber, et al., 2004, p. 8) Structural purpose is actually answered by the previous two features (Webber, et al., 2004, p. 8), thus can be affirmed if they are. The process view on purpose is concerned with the policy outcomes and the way they came to be thus can be operationalized as measures to enhance CIP/CIIP that have been implemented with the incorporation of the private sector. Measures, as pointed out in the previous chapter, can be regulation, information sharing, benchmarking (such as defining minimal standards or best practices) and the use of CERTs. The combination of structural as well as process purpose then denotes the presence of a common

[20] As opposed to the hierarchical relationship envisioned by the state-centrist theories.

purpose. In conclusion, should the features discussed be present in their operationalized form, the hypothesis that the European Union has incorporated the issue of cyberdefense would be confirmed.

EU Defense Policy

The first moves to a common European defense policy actually date back to 1954 with the founding of the West European Union (WEU) (Woyke, 2006a, p. 329). The WEU was created to act as an organization for automatic collective defense, a function that was later delegated to NATO instead. Nonetheless it has existed and even experienced a small revival in the eighties and nineties (Woyke, 2006a, p. 330) until the passing of the Treaty of Lisbon, which incorporated its functions into the general EU framework. The EU itself had been dabbling in the policy field of security policy since the early nineties beginning with the Maastricht Treaty which created the Common Foreign and Security Policy, the second pillar of the former EU structure (Dover, 2009, p. 244). The treaty also stated that the MS should work together to create "a common defence policy and eventually a common defence." (Dover, 2009, p. 245). The time for that policy didn't come however until the Treaty of Nice where the European Security and Defence Policy (ESDP) was introduced. The ESDP gave the EU a military component for the first time in form of the Political and Security Committee and the Military Committee and Staff (Dover, 2009, p. 249). The Petersberg Tasks served as an orientation for the capabilities and missions the EU aspired to (p. 248) and served as framework for the ESDP. Another milestone in European defense policy was the Berlin-plus-agreement which defined its relationship to NATO, as it allowed the EU access to NATO assets and stipulated to avoid duplication institutions and capabilities (p. 249). The Lisbon Treaty served as another stepping stone to further European Defense integration as it made provisions for the MS to react collectively to disasters or terrorist attacks and provided arrangements for greater European military cohesion via the European Defence Agency (Dover, 2009, p. 251).

EU Cyberdefense Activities

The following section will provide an overview of all relevant activities of the European Union in the field of cyberdefense. As previously defined, cyberdefense activities are activities aimed at enhancing security of critical infrastructures and critical information infrastructures when these are concerned with the cyberspace aspect of security. The EU has no formal authority in the field of CIP/CIIP but it has addressed the issue via its competencies in regards to the single market(European Commission, 2009, p. 4). Nonetheless the EU has played an indirect role in CIP/CIIP for some time(Enisa, 2011b) but the current impetus stems from 2004 (cyberthreats weren't mentioned in the European Security Strategy(European Council, 2003)) when the council of ministers asked the commission to prepare an overall strategy for critical infrastructure protection. The Commission responded by referring to regulation already passed in individual sectors as well as to the creation of several relevant agencies.

Further it proposed setting up a European Programme for Critical Infrastructure Protection (EPCIP) and a Critical Infrastructure Warning Information Network (CIWIN)(European Commission, 2004, p. 7). For the EU it also gave a definition of critical infrastructure:

> Critical infrastructure: the physical and information technology facilities, networks, services and assets that, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in EU countries. (European Commission, 2004, p. 3)

This definition shows clearly that the focus of the EU isn't limited to the physical infrastructure but also explicitly addresses the ICT aspect of it. On the onset the efforts for CIP were focused on threats relating to terrorism[21] with but were quickly broadened to a more general effort. Commonly the CIP/CIIP policy is framed as policy relating to the functioning of the single market(EurActiv, 2011), interestingly enough though, documents relating to it are classified in the eur-lex-database as belonging in the "common foreign and security policy"-category[22]. The significance of the ICT sector for the EU has been underlined in several Commission communications as for example the 2006 communication on the secure information society which pointed out that 89% of European companies use the internet for business purposes and that nearly 40% of productivity growth is caused by the ICT sector(European Commission, 2006b).

ENISA 2004

The European Network and Information Security Agency (ENISA) was established in March 2004 by the European Union(European Union, 2004) with the task

> of contributing to a high level of network and information security within the Community and of developing a culture of network and information security for the benefit of citizens, consumers, businesses and public sector organizations in the European Union, thus contributing to the smooth functioning of the internal market..

Its mandate was originally until 2008 but was extended until 2012.It is a community agency(About ENISA, 2011) and not a common foreign and security policy agency(Agencies of the European Union) and focuses on enhancing network and information security in Europe through a variety of activities. Looking at the structure of the agency we can see that it is lead by an executive director and supervised by a management board composed of the representatives of the EU MS, the EU commission and one representative(without voting privileges) each for the ICT industry, consumer groups and academic experts in network and information security(European Union, 2004, Article 6(1)). Further there is the officially established Permanent Stakeholders' Group (European Union,

[21] The Madrid bombings took place in 2004.

[22] See for example (Commission, 2009)

2004, Article 8(1)), which is a panel of experts from the aforementioned groups[23]. It is meant to advise the executive director and be consulted before establishing ad-hoc working groups and drafting the annual work program. An informal institution is the National Liaison Network, established by the executive director, which is compromised by members of the EU and European Economic Area (EEA) MS as wells as the commission and the council(Enisa, 2009a, p. 1; 2011d). The network is used as a means to gain and give input from/to the MS and to facilitate the exchange of best practices(Enisa, 2011d). In addition there is the more general stakeholder management which encompasses all entities, may they be of supranational, international, national or subnational character and from whichever sector, and connects them to the agency (Enisa, 2011c). The work of ENISA is governed by the annual working programs and if one looks at the working programs for the recent years it there are several activities that relate to what was discussed as CIP/CIIP in the previous chapter. Information and Best Practice sharing as wells as stakeholder management is one of the activities that has been continuously carried out from 2005 on. Building trust, technology assessments as well as appraisals of the overall European information and network security level have also been part of the programs for several years. Rather new is the increased interest in CERT cooperation and a very specific CIIP work program. All these measures have been taken in cooperation and consultation with the public as well as the private sector, both of which are incorporated into ENISA by the formal and informal arrangements pointed out above. These work programs[24] show that ENISA is active in the area of CIP/CIIP but that its engagement is also limited to managing networks of relevant actors, developing best practices and enhancing European[25] CIP/CIIP through knowledge transfer. ENISA doesn't possess any regulation capabilities that could be considered "hard law" but it could be argued that it performs "regulation through information"(Majone, 1997, p. 274), for instance when it makes policy recommendations for baseline CERT capabilities(ENISA, 2010a).

EPCIP 2006

In a communication in December 2006 the Commission established a framework to address the issue of infrastructure protection in the EU. The framework consisted of a procedure to identify European Critical Infrastructures (ECI), the decision creation of CIWIN as well as further coordination measures and contingency planning and support for MS for their domestic programs(European Commission, 2006a, pp. 3-4). ECI are defined as those CI whose disruption would affect two or more MS(European Commission, 2006a, p. 4).

[23] See http://www.enisa.europa.eu/about-enisa/structure-organization/psg/members for the current constitution.

[24] See Annex, Table 1

[25] This wording is ambiguous, it is meant as enhancing CIP/CIIP on a national level and therefore also on a European level.

CIIP 2009

In March 2009 the EU Commission published a strategy for CIIP that was endorsed by the member states (MS) later that year. The strategy was proposed in the context of the more general CIP strategy from 2006 and focused on the specific aspects of CIP for CII. The reasoning was that CII played such an important role in the EU but that the national approaches to CIIP varied greatly(European Commission, 2009, p. 5). The strategy seeks to foster a common approach that fosters EU-wider cooperation in this matter and a more European approach in the national policies. It also recognizes the important role the private sector plays in this matter and that market incentives are insufficient to guarantee the desired safety level(European Commission, 2009, p. 6)

Cyber Europe Exercise 2010

On November 4th 2010 the cyber security exercise Cyber Europe 2010 was conducted under the auspices of ENISA with 30 countries participating (all EU member states plus Norway, Switzerland and Iceland). The participants were officials from the respective public sector organizations tasked with CIIP in their home countries, private sector organizations didn't participate (though their participation is planned for further exercises (Saalbach, 2011, p. 24)). The goal of the exercise was to facilitate cooperation between the different national authorities in case of Europe-wide emergencies. To achieve that several scenarios were simulated that forced the participants to act together. According to ENISA the exercise was a success(Trimintzios, Ouzounis, & Siaterlis, 2010, p. 5).

Regulation

The European Union has passed regulation[26] in several areas relevant for CIP/CIIP as for instance in the telecommunication or transportation sector. They are not explicitly termed as CIP but function in the same way as for instance security standards in the ICT sector.

Analysis

The question is if the portrayed efforts by the EU can be considered an incorporation of cyberdefense. To determine this, the analytical framework of security governance devised above will be applied. The framework determines five features that constitute a form of security governance the first of which is a heterarchical relationship between the actors represented. The presence of a heterarchical relationship can be assumed for EU governance in general (George, 2005, p. 125; Marks, et al., 1996, p. 372; Rosamond, 2009, p. 115) but what about the prime example for incorporation, ENISA? Here one can see too, that many different actors have been assembled from the supranational commission over the member states to the representatives of industry, society and academics. The picture is somewhat differentiated by looking at the power structure within ENISA.

[26] A comprehensive list can be found here: (Brunner & Suter, 2008, p. 478)

The central authority, the management board, is composed of a variety of actors from all levels and sectors but voting power rests only with the MS and the commission. However voting procedures call for a simple or 2/3 majority(European Union, 2004, Article 6(4)) and as the commission has a vote the relationship between the actors can't be considered hierarchical in the state-centrist sense. Further there is the presence of two networks of experts that influence the activities and the working program that consist of actors below the level of the nation state which are not on par with the boards members power wise but still are active actors within the framework of ENISA.

This partly answers the second requirement already that a large number of actors need to be involved. As for the European Union, one can make the case that 29 actors are present just by the structure of the Union and that ENISA as an independent agency counts as the thirtieth thus already fulfilling this condition. There are obviously more actors present if one counts for instance the professional association such as the Business Software Alliance(European Commission, 2011) which is active in the field. To turn again to ENISA, taking the management board alone would amount to more than 29 actors and in connection with the formal and informal networks this requirement would be satisfied. In addition there are those actors that are incorporated through the general stakeholder management. Thusly the second requirement can also be seen as satisfied.

Formal and informal arrangements for regulating and coordinating the issue of CIP/CIIP can be found on the EU level and to a lesser extent in the form of ENISA. The EU has obviously formal arrangements that allow it to regulate policy issues within its domain and the institutional setup of council, commission and parliament qualifies as a coordinating mechanism. However formal regulation of CIP/CIIP has been minimal. There have been a number of directives (European Union, 2004, Articles 5-9) that affect the issue but their regulation was done outside a specific CIP/CIIP framework. On the other hand ENISA can be seen as a piece of hard legislation, despite the fact that in itself it represents more a means to enhance CIP/CIIP than setting standards. As such however it can count as one of the informal arrangements for regulation, as the agency itself has not formal regulatory capacity but employs some methods that echo those of the OMC(Warleigh-Lack & Drachenberg, 2009, p. 220). ENISA has for instance published minimal standards for government CERTs and has taken stock of national policies(Enisa, 2011e) and subsequently devised some best practices. This approach by the EU is certainly grounded in the fact that it has no formal authority in the policy field but rather deals with the topic via its authority for the functioning of the single market. ENISA on its own has a variety of coordination arrangements via its permanent stakeholders' group, its management board or its ad-hoc working groups but it has no formal regulation power. Informally as previously mentioned its setting of standards and stock taking of the status quo as well as making policy recommendations can serve as informal regulation analogous to the OMC and with its stakeholder relations as well as the NLO it has also more informal arrangements for input into its policies and working programs.

As pointed out before, the fourth feature, the ideational relationship structured by common norms and discourse, can be generally accepted for the EU. Nonetheless the question can still be asked how far this is true for the issue of cyberdefense and indeed this is certainly a weak point. Not so much in the sense that there isn't an ideational relationship since it seems that the MS as well as the EU institutions are very much on the same page but in the sense that network and information security is viewed through the lens of the single market. In that respect the discourse is limited to the relevance of CIP/CIIP for the economic functioning of the EU and not under the broader approach of defense policy. The significance of this may be mitigated though by a fact pointed out in the previous chapter: While cyberwar may be waged by the military, cyberdefense is a domain where the private sector plays a strong role. While it is not a denial of security governance, this fact does prove relevant in terms of viewing European CIP/CIIP governance as formal defense integration.

Lastly the common purpose can be asserted as a structural purpose can be confirmed via the previous two features and the process purpose can be confirmed on the basis of the work programs mentioned above. ENISA has been active over the past years in the field of CIP/CIIP as it has created benchmarks against which national policies and practices can be measured as well as served as a hub of information sharing either directly or through its activities. In nearly all those activities the private sector has been incorporated either through the formal or informal structures. This confirms that there is indeed a common purpose and ultimately also that there is a European security governance in the field of cyberdefense.

Conclusion

This chapter has reviewed the activities of the European Union in the field of CIP/CIIP with the analytical framework provided by the concept of security governance. The hypothesis that the EU has incorporated CIP/CIIP into its policy spectrum can therefore be confirmed and by this thesis' definition also the incorporation of cyberdefense. In how far this incorporation constitutes defense integration in the sense of the CFSP is highly debatable. While there is common purpose to enhance CIP/CIIP across the EU it is framed in terms protecting the functioning of the single market and not as a matter of defense. While with the Treaty of Lisbon EU defense integration is at its highest level yet and a common defense is indeed envisioned the connection hasn't been made. There could be two explanations for that: The ESDP was from the beginning on oriented towards military cooperation on missions outside of EU territory such as peacekeeping and had very little to do with territorial or domestic defense. Second there is the Berlin-plus-agreement which also meant to avoid duplication of assets. As NATO has been very active since 2007 in addressing the issue of cyberdefense as security policy it might be that the EU is trying to avoid the impression that it is competing with

NATO. That said, the whole policy field is still very much in flux and therefore might be best described as “work in progress” as done by Fritzon et al. concerning the general concept of European CI[27] (2007, p. 39). The policy field has definitely been partly integrated on the European Union level and the EU actually pursues policies that on a national level would be considered cyberdefense.

4. A question of Governance: NATO vs. EU

This chapter deals with the second thesis, which proclaims that the EU is more effective in organizing cyberdefense than NATO because of its different governance approach. In order to check this, first the North Atlantic Treaty Organization will be examined and second the principles of governing elaborated upon in the previous chapter will be checked for their effectiveness in addressing the issue of cyberdefense. It should be pointed out, that this analysis is limited to a comparison between the organizational approaches to governance[28]. While relations within NATO are structured according to intergovernmentalism, it may and has been studied with other analytical frameworks such as security governance (Webber, et al., 2004, p. 9) but usually in the larger context of regional, European of global security. The ability of NATO to function as an actor in a larger governance network is not debated as well as the fact that EU and NATO do cooperate on the issue at hand (Nato, 2011b). The analysis therefore only asserts which model of governing is more effective in addressing cyberdefense and doesn’t per se make any recommendations on the architecture of European cyberdefense.

NATO

The North Atlantic Treaty Organization was founded in 1949 as a mutual defense alliance to balance the perceived threat by the Soviet Union and later the Warsaw Pact. After the fall of the iron curtain and the subsequent dissolve of the Soviet Union there was a momentary lack of purpose however with the conference of Rome in 1991 a new strategy paper was developed that put the focus of NATO past the territorial defense and saw it also as an organization of intervention, either with or without UN-mandate (Woyke, 2006b, p. 374). In addition, the inclusion of the former Warsaw Pact states and the Europeanization of NATO was a stated goal. The first out-of-area-mission took place in 1992 in Bosnia and since then the engagement of NATO in the Balkan area has been continuous with its climax in the Kosovo war of 1999[29]. In addition to its Balkan engagement NATO has been very involved in the “War on Terror” declared by the United States. Article V. was invoked for the first

[27] In its general form.

[28] In general governance refers to the theoretical concept, however in this chapter it may also refer to the act of governing. The theoretical model will be referred to as MLG or it will be explicitly stated.

[29] Fought without a UN mandate.

time in NATO history after the 9/11-attacks(Woyke, 2006b, p. 375). This also led to the participation of NATO in the International Stabilization Force Afghanistan.

Cyberdefense activities

NATO has always been active in protecting its own information systems(Nato, 2011b) but has only begun to see cyberwar as a more general threat after the attacks on Estonia in 2007. In its aftermath NATO expanded its focus from the organizational systems to the key information systems of the MS (Nato, 2008, p.47). As a policy measures it referred to best practices sharing as wells as a rapid response team to help MS that are under attack (Nato, 2008). It is noteworthy that the cyber defense is dealt with under article IV. rather than article V. (EurActiv, 2008). The focus on information systems beyond the organizational ones may however have been taken back again (Nato, 2011a). Other measures taken after 2007 were the creation of the Cyber Defense Management Authority (CDMA) and the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). The role of CDMA is to serve as a coordinator for cyberdefense within the alliance and to assist the individual MS in their needs (Nato, 2011b). Its management board is made up of staff from the MS (Nato, 2011b). Nonetheless the MS are ultimately responsible for the security of their CIP/CIIP. The CCD COE is a research and training institution based in Estonia however it is only sponsored by eight NATO nations (Saalbach, 2011, p. 26). The NATO Communication and Information Services Agency (NCSA) is the entity that is tasked with the actual response to cyberattacks as mentioned above (Nato, 2011b). The CDMA and the NCSA form the operational level of NATO cyberdefense while the CCDCOE and the respective planning committees form the strategic level. NATO has organized several collective cyber defense exercises (Saalbach, 2011, p. 26).

Governance

NATO can be described as an intergovernmental organization (Woyke, 2006b, p. 371) as decisions are made by the representatives of the respective governments. A congressional research report has pointed out, that despite the intergovernmental approach unanimity isn’t always required as there is the concept of “silent consensus” where not an active approval is necessary but an active objection (Gallis, 2003, p. 2). There is a division in a military and a civilian component of which the civilian (or political) component is the policy determining is. Decisions are made by the North Atlantic Council (NAC) as the prime executive organ and this holds also true for the issue of cyberdefense. Other important actors are the Defence Policy and Planning Committee (DPPC) and the NATO Consultation, Command and Control Agency (NC3A) which both serve in an advisory role to the NAC. Both the NC3A and the DPPC are staffed by either personnel by the MS or by international staff. There are no mechanism to punish non-compliance (Ojanen, 2006, p. 73). In general the NATO either hires its own staff or gets staff delegated from the MS and unlike in the EU the decisive management positions such as the NAC or the planning committees are usually made up by national delegates.

Synopsis

NATO has picked up on the issue of cyberdefense earlier than the EU but also with a smaller scope. After the cyberattacks on Estonia however NATO capabilities have been greatly increased. The issue of cyberdefense is dealt with by several authorities within NATO and true to its intergovernmental nature, they are made up of personnel delegated by the MS or hired for NATO itself. There are no actors from the private sphere[30] present and decisions are taken if not by unanimity then at least by consensus without active objections.

Modus Operandi

This section focuses on the comparison of the approaches of intergovernmentalism and multi-level governance to the issue of cyberdefense. The judgment shall be made which approach to governing is more effective in addressing the challenges of cyberwar, the governance approach of the EU or the intergovernmentalism by NATO. However, before coming to that judgment there is the need to clarify what is meant by more effective.

What is needed for effective cyberdefense?

When looking at NATO and the EU, one sees an organization that for decades was the cornerstone of European security policy and an organization that has for the majority of its existence focused more on the economic aspects of European cohabitation[31]. The question is then, why today the traditionally non-military organization should be more adept in dealing with new security threats than the old one and the answer, according to the hypothesis, lies in its governing principles. The assumption is that MLG is more effective in addressing the characteristics of cyberwar than intergovernmentalism. Obviously the term “effective” is questionable, as it is devoid of meaning on its own but the suggestion is to view effectiveness in terms of the ability to address the characteristics of cyberwar better. Recalling chapter two, the characterization of cyberwar and subsequently cyberdefense brought some fundamental differences in comparison to traditional warfare to light. Key differences are the role private actors play and the increasing interconnectedness of infrastructure. By that characterization, to evaluate the effectiveness of the two approaches to governing is to ask how well they can incorporate private actors and address the issue of interdependency via their respective modi operandi. To be more specific the questions

[30] The exception is most likely the defense procurement division but that is of no relevance here.

[31] Admittedly the European Communities were founded to prevent further conflicts like WWI&II and have so far been very successful at that, nonetheless the focus for the majority of its existence so far has only indirectly been on security.

discussed will be how well the intergovernmentalism of NATO and the MLG of the EU incorporate the private sector into the decision and debating mechanisms and in the implementation supervision. The second question should be, considering the diagnosed differences in the approaches and standards of CIP/CIIP (European Commission, 2009, Point 3.4.1), how the governing approach can ensure more uniform standards and policies to address the issue of increasing interdependence of European critical infrastructure.

Intergovernmentalism vs. MLG

As for the integration of the private sector, the approach taken by intergovernmentalism is very clear: there is no incorporation on the supranational level. This is posited by liberal intergovernmentalism and it seems to be echoed by the actual proceedings in NATO. On the domestic level private actors can play a role, but above that level there is only the state as unitary actor. This is also seen in the policy that MS are responsible for their CIP/CIIP and in case of need are supported by NATO CERTs. While NATO does use best practice sharing, this again is done at the state level and not between CIP/CIIP operators. MLG is taking a very different approach in theory and as exemplified by the EU. Actors can cooperate freely (in theory) and actually do so to some extent (in practice). While nation states and the supranational institutions of the EU are the key players, when it comes to CIP/CIIP, there are numerous ways that the private sector is connected to the policy process. ENISA as the prime actor within the EU for CIP/CIIP has incorporated the private sector in its policy and program consideration through the networks it manages. There however no integration when it comes to implementation supervision, which is partly because so far there are few concrete measures. Theoretically there is the possibility though, especially since ENISA has chosen some approaches like best practice sharing or benchmarking that do reflect suggestions by academic authors for integrating the private sector.

While both governing approaches do incorporate the private sector somehow, MLG does so far more comprehensively. For intergovernmentalism there is always the state government as a “bottleneck” for inclusion in supranational policy-making. While it doesn’t prevent the private actors from shaping government positions domestically, it has been pointed out that interests of the state and the business sector are likely to have diverging interests. How far the positions of the latter can and will be represented by the state is questionable. In a system of MLG the private sector can interact with the public sector at any level and this is seen by the example of ENISA and the EU.

How then, can the two approaches ensure a more uniform policy across Europe? Intergovernmentalism in theory can do so very well, at least in its liberal form. Treaties on security policy like disarmament treaties or the Geneva Convention have been successfully adopted. A problem however lies in securing the implementation and its verification (Baylis, 2006, p. 304). If there are no sanctions available to punish dissent then implementation might not as rigorous as expected. Essentially this refers to the problem of non-compliance. NATO itself has no arrangements for sanctions and disputes are dissolved by inter-state diplomacy. Conceptually the decision-making process should lead to policy outcomes that all states want to implement but with silent consensus procedure this may not always be the case (Gallis, 2003, p. 2). Another limitation for NATO is obviously its rather narrow focus on security and defense matters which in the case of cyberdefense leave relevant policy field outside of the scope of NATO. As defense in cyberwar depends highly on the private sector, the missing authority of NATO pertaining to the regulation of this sector is a serious detriment. MLG like intergovernmentalism can adopt regulation at a supranational level and thus provide a uniform framework across all national and private actors. Unlike intergovernmentalism it isn't dependent on unanimity but can adopt policy even if some countries abstain or object, thus giving it the possibility to enforce standards that are in the interest of the (qualified-) majority. However there is also the question of non-compliance[32]. An advantage here is though, that with the incorporation of the private sector and without the compartmentalization into nation states, the verification is easier. As mentioned in the first chapter, the control of businesses is sometimes more effective through other businesses. In the specific case of the EU, there are institutionalized sanction mechanisms that can be called upon by all actors. What's more the EU has authority over a wide variety of policy fields and in the context of the single market can pass far reaching regulation of the private sector. On the other hand though, the access to the field of defense and security policy is still limited, forcing the EU to address cyberdefense through policy that is officially related to the economic well-being.

In the end, what speaks for MLG is, that when it comes to CIP/CIIP, the verification of policy implementation is potentially a lot better than under intergovernmentalism due to the incorporation of more actors and especially the private sector.

Conclusion

Thus MLG can be considered more effective in addressing the challenges of cyberdefense. However that is not to say that intergovernmentalism is inept but as a governance approach it depends very much on the specific practical arrangements. The key advantage of MLG is its ability to incorporate more actors into the policy process which, considering the importance of the private sector in CIP/CIIP, is crucial. On a practical level the institutional arrangements by the EU provide a better implementation control and when it comes to regulating the private sector (in cooperation or not) the EU has a wider array of policy fields and instruments at its hand.

[32] See (Treib, 2006) for an overview of theory and practice.

6. Conclusion

This thesis set out to look into the topic of European cyberdefense. Accordingly, the second chapter investigated the concept of cyberwar and found that by the term is meant the deliberate attack on critical infrastructure. In reverse, this means that cyberdefense must address the issue of CIP/CIIP. Following this excursion the two hypotheses that were posited were tested.

The first proclaimed that the EU has already incorporated cyberdefense and was tested via the analytical framework of security governance. The presence of a distinct set of institutional arrangements with the purpose of CIP/CIIP were found and therefore the presence of a form of security governance in the field confirmed. Thus it is fair to say that the EU has integrated cyberdefense as a policy field even though one should point out that the integration is still in flux and that it isn't addressed through the ESDP but through the EU authority over the functioning of the single market.

The second hypothesis stated that the EU is better suited to organize a European cyberdefense on account of its governance approach in comparison to NATO. To test this, the two approaches to governing, MLG and intergovernmentalism, were analyzed in regard to their capability to address the challenges posed by cyberwar in contrast to traditional warfare. MLG did prevail on account of its ability to incorporate a wider array of actors into the policy process, which can indeed be considered true for the EU. On the practical level, the institutional arrangements of the EU also facilitated CIP/CIIP. However, it was also pointed out, that intergovernmentalism isn't unfit for the task but that it depends very much on the practical implementation of structures.

Both hypotheses address in their way, the discourse on the future European security architecture and contemplating their implications for a moment might be interesting. The first thesis did confirm that the EU is active in a policy field that has the potential of becoming very important in terms of its security implications in the future and the second hypothesis can be seen to support this as the EU might be better suited to deal with it than NATO. A slight confirmation of this may be the fact that NATO policy concerning cyberdefense was supposedly changed to a narrower approach than before (Nato, 2011a) but as this has happened only very recently it is too soon to be confirmed. In addition, there is no reason to believe that security provision in Europe should become the uncontested domain of one organization after the decades of parallel structures and cooperation and competition. The field of cybersecurity, in general, and cyberdefense, in particular, may nonetheless be an area where the EU can find a role as a security actor in the future. Considering the call for a common defense has been uttered more than once, cyberdefense may be the right point to start. This thesis attests at least that the foundation is there and that governance-wise, the EU may have an edge over NATO.

Bibliography

Abele-Wigert, I. (2006). Challenges Governments Face in the Field of Critical Information Infrastructure Protection (CIIP): Stakeholders and Perspectives. In M. Dunn Cavelty & V. Mauer (Eds.), *International CIIP Handbook 2006* (Vol. II, pp. 55-68). Zurich: Center for Security Studies, ETH Zurich.

. About ENISA. (2011) Retrieved 08.03.2011, from http://www.enisa.europa.eu/about-enisa

. Agencies of the European Union. Retrieved 08.03.2011, 2011, from http://europa.eu/agencies/index_en.htm

Arnett, E. H. (1992). Welcome to hyperwar. *BULLETIN-ATOMIC SCIENTISTS, 48*, 14-14.

Aronson, J. D. (2006). Causes and consequences of the communication and Internet revolution. In J. Baylis & S. Smith (Eds.), *The Globalization of World Politics. An introduction to international relations* (3rd ed., pp. 621-644). Oxford: Oxford University Press.

Arquilla, J., & Ronfeldt, D. (1993). Cyberwar is coming! *Comparative Strategy, 12*(2), 141-165.

Azarov, S. S., & Dodonov, A. G. (2003). *INSTRUMENTAL CORRECTIONS FOR A DEFINITION OF CYBERWAR.* Paper presented at the NATO Advanced Research Workshop on Cyberwar-Netwar, Lisbon.

Baylis, J. (2006). International and Global Security in the Post-Cold War Era. In J. Baylis & S. Smith (Eds.), *The Globalization of World Politics. An introduction to international relations* (3rd ed., pp. 297-324). Oxford: Oxford University Press.

Bendrath, R., Eriksson, J., & Giacomello, G. (2007). From 'cyberterrorism'to 'cyberwar', back and forth. In J. Eriksson & G. Giacomello (Eds.), *International relations and security in the digital age* (pp. 57-82). Abingdon: Routledge.

Brunner, E. M., & Suter, M. (2008). *International CIIP Handbook 2008/2009*. Zurich: Center for Security Studies, ETH Zurich.

Catteddu, D. (2011). Protecting European Critical Information Infrastructures *Europe Today,* (12/2010), 15. Retrieved from http://www.europaeische-akademie.eu/fileadmin/user_upload/dateien/Europe_Today/articles/Protecting_European_Critical_Information_Infrastructures.pdf

Cini, M. (2009). Intergovernmentalism. In M. Cini & N. Pérez-Solórzano Borragán (Eds.), *European Union Politics* (pp. 86-103). New York: Oxford University Press.

Coen, D., & Thatcher, M. (2008). Network governance and multi-level delegation: European networks of regulatory agencies. *Journal of Public Policy, 28*(01), 49-71.

Collier, S., & Lakoff, A. (2008). The Vulnerability of Vital Systems: How ''Critical Infrastructure''Became a Security Problem. *Securing the Homeland: Critical Infrastructure, Risk, and (In) Security, edited by M. Dunn-Cavelty and K. S. Kristensen. London: Routledge*.

Commission, E. (2009). EUR-Lex - CIIP Communication Retrieved 11.03.2011, from http://eur-lex.europa.eu/Notice.do?checktexts=checkbox&val=493232:cs&pos=1&page=1&lang=en&pgs=10&nbl=1&list=493232:cs,&hwords=&action=GO&visu=#texte

Cornish, P., Livingstone, D., Clemente, D., & Yorke, C. (2010). On Cyber Warfare *A Chatham House Report*: Chatham House.

. Cyberwarfare: Marching off to cyberwar. (2008). *The Economist* Retrieved 06.03.2011, from http://www.economist.com/node/12673385

Donahue, J. D., & Zeckhauser, R. (2006). Sharing the Watch: Public-Private Collaboration for Infrastructure Security. In P. E. Auerswald, L. M. Branscomb, T. M. La Porte & E. O. Michel-Kerjan (Eds.), *Seeds of Disaster, Roots of Response* (pp. 429-456). Cambridge: Cambridge University Press.

Donahue, J. D., & Zeckhauser, R. (2008). Public-Private Collaboration. In M. Moran, M. Rein & R. E. Goodin (Eds.), *The Oxford Handbook of Public Policy.* (pp. 496–525). Oxford: Oxford University Press.

Dover, R. (2009). From CFSP to EDSP: the EU's Foreign, Security and Defense Policies. In M. Cini & N. Pérez-Solórzano Borragán (Eds.), *European Union Politics* (pp. 239-257). New York: Oxford University Press.

Dunn-Cavelty, M. (2005). The socio-political dimensions of critical information infrastructure protection (CIIP). *International Journal of Critical Infrastructures, 1*(2), 258-268.

Dunn-Cavelty, M. (2008a). *Cyber-security and threat politics: US efforts to secure the information age*. London: Routledge.

Dunn-Cavelty, M. (2008b). Like a phoenix from the ashes. In M. Dunn-Cavelty & K. S. Kristensen (Eds.), *Securing'the homeland': critical infrastructure, risk and (in) security* (pp. 40). London: Routledge.

Dunn-Cavelty, M. (2010). Cyberwar: Concepts, Status Quo, And Limitations *CSS Analysis in Security Policy* (Vol. 71). Zurich: Center for Security Studies, ETH Zurich.

Dunn-Cavelty, M., & Brunner, E. M. (2007). Introduction: Information, Power, and Security - An Outline of Debates and Implications. In M. Dunn-Cavelty, V. Mauer & S. F. Krishna-Hensel (Eds.), *Power and Security in the Information Age* (pp. 18). Hampshire: Ashgate Publishing Limited.

Dunn-Cavelty, M., & Kristensen, K. S. (2008). Introduction. In M. Dunn-Cavelty & K. S. Kristensen (Eds.), *Securing'the homeland': critical infrastructure, risk and (in) security* (pp. 14). London: Routledge.

Dunn-Cavelty, M., & Suter, M. (2009). Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection. *International Journal of Critical Infrastructure Protection, 2*(4), 179-187.

Enisa. (2005). *Working Programme 2005*. Enisa.

Enisa. (2006). *Working Programme 2006*. Enisa.

Enisa. (2007). *Working Programme 2007*. Enisa.

Enisa. (2008). *Working Programme 2008*. Enisa.

Enisa. (2009a). ENISA Relations with EU Bodies & Member States Retrieved 11.03.2011, from http://www.enisa.europa.eu/media/key-documents/fact-sheets/Member_States-1.pdf

Enisa. (2009b). *Working Programme 2009*. Enisa.

ENISA. (2010a). Baseline Capabilities of National / Governmental CERTs: ENISA.

Enisa. (2010b). *Working Programme 2010*. Enisa.

Enisa. (2011a). CERT Retrieved 08.03.2011, from http://www.enisa.europa.eu/act/cert

Enisa. (2011b). Legal References Retrieved 08.03.2011, from http://www.enisa.europa.eu/about-enisa/regulatory-framework/legal-references

Enisa. (2011c). Managing Relationships Retrieved 11.03.2011, from http://www.enisa.europa.eu/act/sr/networks

Enisa. (2011d). NLO Network Retrieved 11.03.2011, from http://www.enisa.europa.eu/about-enisa/structure-organization/national-liaison-office

Enisa. (2011e). Stock Taking of National Policy and Regulatory Environments Retrieved 12.03.2011, from http://www.enisa.europa.eu/act/res/policies/stock-taking-of-national-policies

Enisa. (2011f). *Working Programme 2011*. Enisa.

Eriksson, J., & Giacomello, G. (2007). Digital-age security in theory and practice. In J. Eriksson & G. Giacomello (Eds.), *International relations and security in the digital age* (pp. 173-184). Abingdon: Routledge.

Esterle, A., Ranck, H., & Schmitt, B. (2005) Information Security: A new challenge for the EU. *Vol. 76*. Paris: Institute for Security Studies.

EurActiv. (2008). NATO agrees common approach to cyber defence Retrieved 12.03.2011, from http://www.euractiv.com/en/infosociety/nato-agrees-common-approach-cyber-defence/article-171377

EurActiv. (2011). Problemfälle: Cyberwar, Nahost, Ägypten, Afghanistan Retrieved 10.03.2011, from http://www.euractiv.de/sicherheit-und-verteidigung/artikel/problemfalle-cyberwar-nahost-afghanistan-004325

European Commission. (2004). *Critical Infrastructure Protection in the fight against terrorism* (702).

European Commission. (2006a). *Communication from the Commission on a European Programme for Critical Infrastructure Protection* (COM(2006) 786). European Commission.

European Commission. (2006b). *A strategy for a Secure Information Society - "Dialogue, partnerhsip and empowerment"*. European Commission Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0251:FIN:EN:PDF.

European Commission. (2009). *"Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience"* European Commission.

European Commission. (2011). Business Software Alliance. from European Commission https://webgate.ec.europa.eu/transparency/regrin/consultation/displaylobbyist.do?id=7503 9383277-48

European Council. (2003). *A Secure Europe in a Better World: European Security Strategy*. (702).

Regulation (EC) No460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (2004).

Fogleman, R. (1995). Information Operations: The Fifth Dimension of Warfare Retrieved 06.03.2011, from http://www.iwar.org.uk/iwar/resources/5th-dimension/iw.htm

Fritzon, Å., Ljungkvist, K., Boin, A., & Rhinard, M. (2007). Protecting Europe's Critical Infrastructures: Problems and Prospects. *Journal of Contingencies and Crisis Management, 15*(1), 30-41.

Gallis, P. (2003). *NATO's Decision-Making Procedure*. (RS21510). Washington D.C.: U.S. Congressional Research Service.

George, S. (2005). Multi-level Governance and the European Union. In I. Bache & M. Flinders (Eds.), *Multi-level Governance* (pp. 107-126). Oxford: Oxford University Press.

Gibson, W. (1984). *Neuromancer*: Ace.

Hunker, J. (2010). Cyber war and cyber power. *Research Paper, 62*, 12. Retrieved from

Jachtenfuchs, M. (2005). Intergouvernrmentalismus. In D. Nohlen & R.-O. Schultze (Eds.), *Lexikon der Politikwissenschaft* (3rd ed., Vol. 1, pp. 400-401). München: Verlag C.H.Beck.

Jordan, A. (2001). The European Union: an evolving system of multi-level governance... or government? *Policy & Politics, 29*(2), 193-208.

Lewis, J. A. (2009). The" Korean" Cyber Attacks and Their Implications for Cyber Conflict. *Center for Strategic and International Studies, Washington, DC*.

Libicki, M. C. (1995). *What is information warfare?* : Center for Advanced Concepts and Technology, Institute for National Strategic Studies, National Defense University.

Libicki, M. C. (2009). *Cyberdeterrence and Cyberwar*. Santa Monica: RAND Corporation.

Lorents, P., Ottis, R., & Rikk, R. (2009). Cyber Society and Cooperative Cyber Defence. *Internationalization, Design and Global Development*, 180-186.

Majone, G. (1997). The new European agencies: regulation by information. *Journal of European Public Policy, 4*(2), 262 - 275.

Marks, G., Hooghe, L., & Blank, K. (1996). European integration from the 1980s: State-centric v. multi-level governance. [Article]. *Journal of Common Market Studies, 34*(3), 341.

Metz, S., & Kievit, J. (1995). Strategy and the Revolution in Military Affairs: From Theory to Policy: Strategic Studies Institute, Army War College.

Nato. (2008). NATO Summit Bucharest 2008 Retrieved 12.03.2011, from http://www.summitbucharest.ro/en/doc_201.html

Nato. (2011a). Defence Ministers approve Cyber Defence Concept Retrieved 14.03.2011, from http://www.nato.int/cps/en/SID-A2672ABB-BECFFD6A/natolive/news_71432.htm?selectedLocale=en

Nato. (2011b). NATO - Topic: Cyber attacks, Defending against Retrieved 14.03.2011, from http://www.nato.int/cps/en/natolive/topics_49193.htm

Ojanen, H. (2006). The EU and NATO: Two competing models for a Common Defence Policy. *JCMS: Journal of Common Market Studies, 44*(1), 57-76.

Ottis, R. (2008). *Analysis of the 2007 cyber attacks against Estonia from the information warfare perspective.* Paper presented at the Proceedings of the 7th European Conference on Information Warfare, Plymouth.

Ottis, R., & Lorents, P. (2010). *Cyberspace: Definition and Implications*. Paper presented at the 5th International Conference on Information Warfare and Security, Dayton, OH.

Reich, P. C., Weinstein, S., Wild, C., & Cabanlong, A. S. (2010). Cyber Warfare: A Review of Theories, Law, policies, Actual Incidents - and the Dilemma of Anonymity. *European Journal of Law and Technology, 1*(2), 58.

Rona, T. P. (1976). *Weapons Systems and Information War*. (84-0778). Washington D.C.: Department of Defense Retrieved from http://www.dod.gov/pubs/foi/reading_room/09-F-0070WeaponSystems_and_Information_War.pdf.

Rosamond, B. (2009). New Theories of European Integration. In M. Cini & N. Pérez-Solórzano Borragán (Eds.), *European Union Politics* (pp. 104-122). New York: Oxford University Press.

Saalbach, K. (2011). Cyberwar-methods-and-practice: University of Osnabrück.

Shimeall, T., Williams, P., & Dunlevy, C. (2001). Countering cyber war. *NATO Review, 49*(4), 16-18. Retrieved from http://www.nato.int/docu/review/2001/0104-04.htm

Sommer, P., & Brown, I. (2011). Reducing Systemic Cybersecurity Risk *Future GLobal Shocks* (pp. 119): OECD.

Strate, L. (1999). The varieties of cyberspace: Problems in definition and delimitation. *Western journal of communication, 63*(3), 382-412.

Stroby Jensen, C. (2009). Neo-functionalism. In M. Cini & N. Pérez-Solórzano Borragán (Eds.), *European Union Politics* (pp. 71-85). New York: Oxford University Press.

Submarine Cable Map. (2011). PriMetrica Inc.

The Economist. (2010a). The meaning of Stuxnet. *The Economist*. Retrieved from http://www.economist.com/node/17147818/print

The Economist. (2010b). The Stuxnet outbreak: A worm in the centrifuge. *The Economist*. Retrieved from http://www.economist.com/node/17147818/print

The Economist. (2010c). The Stuxnet worm: Yet to turn. Retrieved from www.economist.com website: http://www.economist.com/node/17730556?story_id=17730556

Treib, O. (2006). Implementing and complying with EU governance outputs. *Living Reviews in European Governance, 1*(1), 2006-2001.

Trimintzios, P., Ouzounis, E., & Siaterlis, C. (2010). CYBER EUROPE 2010: First Ever Pan-European Exercise on Large Scale ICT Incidents. *ENISA Quarterly Review, 6*(4), 3-5. Retrieved from http://www.enisa.europa.eu/publications/eqr/issues/eqr-q4-2010-vol.-7-no.-4/at_download/issue

Warleigh-Lack, A., & Drachenberg, R. (2009). Policy Making in the European Union. In M. Cini & N. Pérez-Solórzano Borragán (Eds.), *European Union Politics* (pp. 209-224). New York: Oxford University Press.

Webber, M., Croft, S., Howorth, J., Terriff, T., & Krahmann, E. (2004). The governance of European security. *Review of International Studies, 30*(01), 3-26.

Wilson, C. (2007). *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*. (RL32114). Washington D.C.: U.S. Congressional Research Service.

Woyke, W. (2006a). Militärbündnisse. In W. Woyke (Ed.), *Handwörterbuch Internationale Politik* (pp. 326-333). Bonn: Bundeszentrale für politische Bildung.

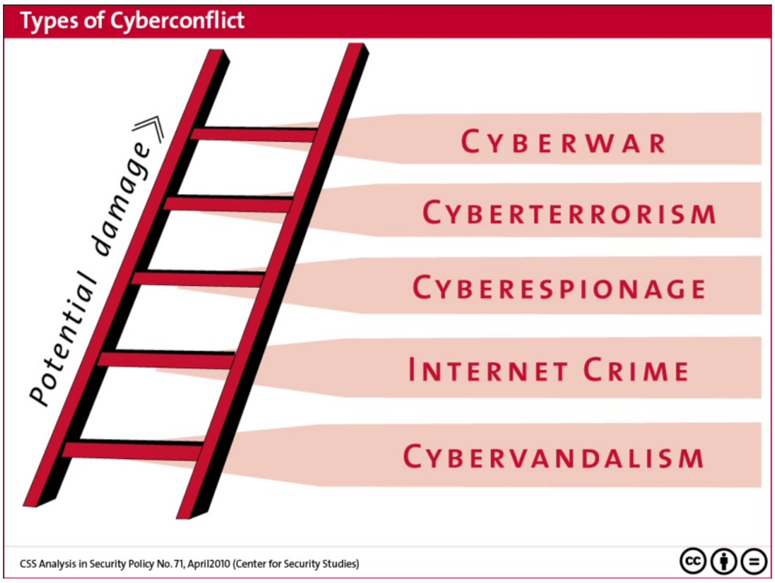
Woyke, W. (2006b). NATO. In W. Woyke (Ed.), *Handwörterbuch Internationale Politik* (pp. 369-378). Bonn: Bundeszentrale für politische Bildung.

Zuckerman, E., Roberts, H., McGrady, R., York, J., & Palfrey, J. (2010). 2010 Report on Distributed Denial of Service (DDoS) Attacks: Berkman Center for Internet & Society.

Annex

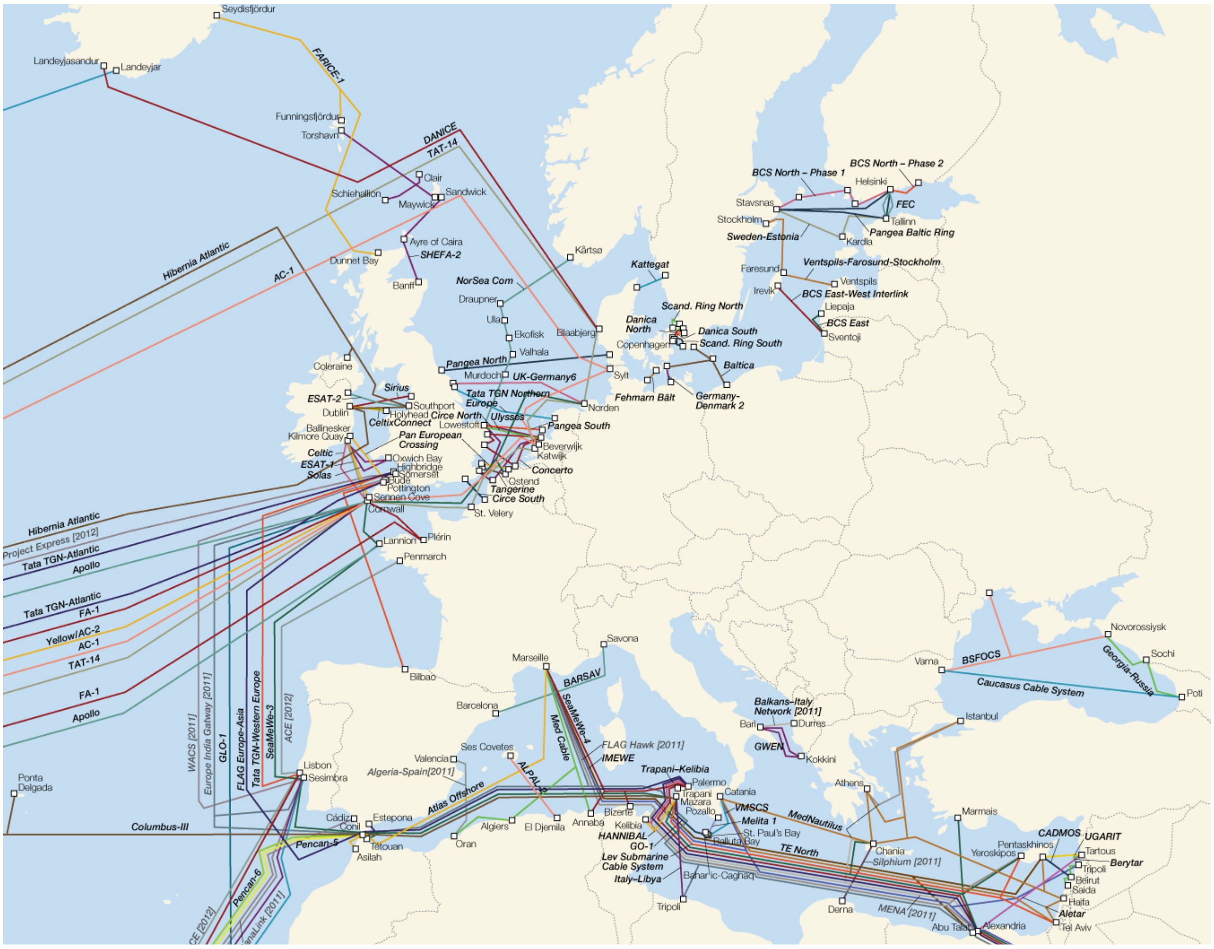
WP	2005[33]	2006[34]	2007[35]	2008[36]	2009[37]	2010[38]	2011[39]
Building Trust		x	x	x		x	x
Information & Best Practice Sharing	x	x	x	x	x	x	x
Stakeholder Management	x	x	x	x	x	x	x
CERT cooperation				x		x	x
Appraisal of EU security level			x	x	x	x	
Technology Assessment	x	x	x	x		x	x
CIIP				x		x	x

Table 1, own construction



Picture 1, (Myriam Dunn-Cavelty, 2010, p. 2)

[33] See (Enisa, 2005)
[34] See (Enisa, 2006)
[35] See(Enisa, 2007)
[36] See(Catteddu, 2011; Enisa, 2008)
[37] See(Enisa, 2009b)
[38] See(Enisa, 2010b)
[39] See(Enisa, 2011f)



Picture 2, (Submarine Cable Map, 2011)