BACHELOR THESIS ES

The use of Legal Competences for Cyber-security Policy by the EU

Author: Tin Chie Man (1028340) Supervisors: R.A. Wessel / C. Matera

11419 Words

Abstract

In this paper the following question is answered: how can the EU make optimal use of the different legal competences given the internal and external dimension of its cyber-security policy? I will argue that the optimal use of competence for the EU in its current framework, is a coordinating and supporting role in the policy area of cyber-security. The EU's conception of cyber-security shall be clarified and the Pre- and Post-Lisbon situations elaborated.

Table of Contents

1. Introduction

"Over the last two decades, the Internet and more broadly cyberspace has had a tremendous impact on all parts of society." (European Commission, 2013) With these words, the European Commission launched its strategy on cyber-security (Bunker, 2013).

In recent years and especially after the revelations about cyber intelligence gathering by American intelligence services in June 2012, the discussion about privacy and cyber-security had been intensified throughout the world. People started to realize how important cyber-security was. States were probably already aware of the importance of cyber-security, but were given a wake-up call nonetheless. Tackling the problem nationally, however, proved to be rather problematic because nations have large differences in approaches to cyber-security (Luiijf, Besseling, & de Graaf, 2013)

Cyber-security is no longer or perhaps has never been a problem on a national scale. Nearly all elements in cyber space cross borders. Therefore, the EU as the most important international organization in Europe, is an important actor in solving cyber-security problems. Before the introduction of the Lisbon Treaty in 2009 cyber-security issues were divided between the three Pillars of the Union: the European Communities (EC), Common Foreign and Security Policy (CFSP) and the Police and Judicial Co-operation in Criminal Matters (PJCC).

The reform of the Pillar structure by the Lisbon Treaty paved the way for a unified cyber-security policy in the EU. In 2013 this was realized in the 'Cyber-security Strategy' and 'Directive Proposal' (European Commission, 2013). Although the new EU structure gave much needed uniformity to the cyber-security strategy, some 'loose ends' still remain in the form of *"…unresolved and undefined competences."* (Dewar, 2015) An example is external cyber-security policy relating to the CFSP. These 'loose ends' have resulted in a *"…grey area of policy, which translates into an institutionalised complexity of responsibilities and action…"* (Dewar, 2015) where competences of the EU are unclear.

On top of this, the EU's conception of cyber-security is rather broad. Not only does it want to safeguard access and openness and maintain reliability and interoperability, but it also aims to protect fundamental rights, democracy and the rule of law in cyberspace. Due to the large scope of the conception, cyber-security policy of the EU involves many areas including, but not limited by the Area of justice, freedom and security, internal market, research and innovation and the abovementioned CFSP. (European Commission, 2013)

So the EU has ambitions on cyber-security on the one hand and cloudy competences on the other hand. This sparks the discussion on how the EU should use its available legal tools and whether it should change the Treaties in order to challenge the problems.

In this paper, the legal competences that the EU can use to reach its digital security objectives will be examined. The following main question will be answered: How can the EU make optimal use of the different legal competences given the internal and external dimension of its cyber-security policy?

The main question shall be answered using the following sub-questions:

- 1. What is the EU's conception of cyber-security?

- 2. In which way has the EU so far regulated the policy area?

1.1 Methodology

In the first section I explore what the EU's conception of cyber-security is. In order to understand what it entails, I started by taking a closer look at how Nissenbaum framed computer security in 2005. Arguing which conception of cyber-security most correctly describes it goes beyond the scope of this paper and therefore shall not be discussed. Also, the objective of this thesis is not to figure out all the conceptions of cyber-security. Therefore, Nissenbaum was chosen because her two conceptions clearly show a contrast between what is regarded as 'technical computer security' and 'cyber-security'.

Following this, I explore the EU's conception on cyber-security. This is done by analyzing EU policy documents, mainly its 2020 Digital Strategy. Finally, an example is given on how 'cyber-security' is framed by an international organization other than the EU: the United Nations (UN). This is done by analyzing reports and resolutions made by expert groups of the General Assembly of the UN in the Field of Information and Telecommunications in the Context of International Security.

The third section encompasses the main body of my Bachelor thesis. The relationship between cyber-security and objectives of the EU are investigated. Cyber-security policy and regulation Pre- and Post-Lisbon is mapped out by looking at EU Treaty Articles and policy documents such as Communications, Regulations, Directives and Strategies. It is not the objective of this paper to map out all measures in cyber-security policies. Instead, the legal basis where these policies are based upon and the competences are more relevant. A distinction is made between internal and external policy. Particular attention shall be paid to the Common Foreign and Security Policy (CFSP) and CSDP because they form an integral part of the EU's external action. The use of competences by the EU and its flaws in the area of cyber-security will be analyzed.

The conclusion will answer the research question: How can the EU make optimal use of the different legal competences given the internal and external dimension of its cyber-security policy?

1.2 Relevance

By answering these questions, the study will give a better insight in the tensions between the EU's ambitious internal and external cyber-security policies and the legal competences of the EU. With a more complete understanding of competences, subsequently, EU policy makers can take away the tensions by adjusting legislation and/or policies thus resulting into a more effective cyber-security strategy.

2. The EU's conception of 'cyber-security'

In order to be able to analyze the relationship between cyber-security and the EU, one must first know what the EU's conception of 'cyber security' entails. The concept of cyber-security has evolved in a fast pace alongside cyberspace in the last decades, but still remains undefined and complicated. (Kruger, 2014) As a result of this lack of clarity, it is a great challenge for the EU to create new legislation in this area.

Indeed*, "…the relative fuzziness of the definitions as well as the broad scope of the area that will also make it more difficult to take new legislative initiatives in the appropriate EU policy fields."* (Wessel, Towards EU Cybersecurity Law: Regulating a New Policy Field, 2015 (forthcoming)) As Wessel sums it up, the broad scope of the area and fuzziness of the definitions are quite problematic for the creation of new legislative initiatives.

2.1 Nissenbaum

The broad scope of cyber security can be illustrated on the basis of Nissenbaum's conceptions. She claimed in 2005 that there were two dominant conceptions of computer security: 'technical computer security' and 'cyber-security'. The two notions, although contrasting, are not entirely conflicting with each other. Both have a different origin according to Nissenbaum. Technical computer security has its origin in *"…individual-focused conceptions of computer security developed in computer science and engineering."* (Nissenbaum, 2005) Cyber-security was derived from *"…the concerns of national security agencies of government as well as those of corporate intellectual property owners."* (Nissenbaum, 2005)

2.1.1 Technical computer security

The former is a more traditional conception focusing *"…on protecting computer systems and their users against attacks, and threats of attack…"* (Nissenbaum, 2005) There is a distinction in three categories of attacks: *"Attacks that render systems, information, and networks unavailable to users,… Attacks that threaten the integrity of information or of systems and networks…* [and] *Attacks that threaten the confidentiality of information and communications,…"* (Nissenbaum, 2005) Nissenbaum claims that the categories are still applicable even though attacks have changed over time. New defenses have emerged to counter new types of attack. Yet the conception of 'technical computer security' is still focused *"…on protection against deliberate attack."* (Nissenbaum, 2005)

2.1.2 Cyber-security

Nissenbaum's latter conception 'cyber-security' has, similar to technical computer security, divided threats into three categories: *"Threats posed by the use of networked computers as a medium or staging ground for antisocial, disruptive, or dangerous organizations and communications…Threats of attack on critical societal infrastructures,…* [and] *Threats to the networked information system itself ranging from disablement of various kinds and degrees to – in the worst case – complete debility."*

The foremost difference is that Nissenbaum's cyber-security has a larger scope than technical computer security. For example, more and more nations use cyberspace to keep their citizens in check. To prevent the abuse of cyberspace for this purpose, freedom and fundamental rights of individuals should be protected online. (European Commission, 2013) Other possible reasons for respecting human rights and freedoms in cyberspace include but are not restricted to preventing breaches of privacy by individuals, businesses and organizations, spam, racism and xenophobia. (United Nations, 2013)

But scope is not the only distinction. Cyber-security recognizes effects beyond that of an attack itself such as social consequences. In cyber-security, the aftermath of attacks range from damage to property to incursions on privacy, productivity and autonomy. Another difference is the subject that both conceptions are referring to. Technical computer security seeks to protect 'individual nodes' like people, agents and institutions while cyber-security targets the collectives such as nations and states. The third difference highlighted by Nissenbaum are 'sources of moral force' and this relates to the former. Collective security uses different justifications for actions taken than individual security.

2.2 The EU, cyber-security and cybercrime

The second problem is the fuzziness of the definitions. The EU has made cyber-security and cybercrime a part of their policy in the Europe 2020 Strategy. The 2020 strategy has the following structure: three engines divided into seven flagship initiatives. The Digital Agenda for Europe is a flagship initiative which is part of the Smart Growth Engine. The Digital Agenda is divided into seven pillars: I. Digital Single Market, II. Interoperability & Standards, III. Trust & Security, IV. Fast and ultra-fast Internet access, V. Research and innovation, VI. Enhancing digital literacy, skills and inclusion, VII. ICT-enabled benefits for EU society. The third pillar contains cyber-security.

In the previous section, I have explored two dominant conceptions of cyber-security. A concept often associated with it is cybercrime. So how are these two related with each other and how does the EU define them? The EU's 2013 'Cyber-security Strategy' depicts them in this fashion:

"Cyber-security commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber-security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein.

Cybercrime commonly refers to a broad range of different criminal activities where computers and information systems are involved either as a primary tool or as a primary target. Cybercrime comprises traditional offences (e.g. fraud, forgery, and identity theft), content-related offences (e.g. on-line distribution of child pornography or incitement to racial hatred) and offences unique to computers and information systems (e.g. attacks against information systems, denial of service and malware)." (European Commission, 2013)

As you can see, cyber-security is regarded as something that guards the cyber domain against threats, while cybercrime is a part of these threats originating from unlawful actions. Or, as Wessel puts it: *"…while cybersecurity refers to the range of safeguards and actions that can be used to protect the cyber domain, cybercrime reflects to the actual criminal activities, thus following the descriptions laid down in the Council of Europe Convention on cybercrime."* (Wessel, Towards EU Cybersecurity Law: Regulating a New Policy Field, 2015 (forthcoming))

2.3 Criticism on the EU's definition and other key concepts

The EU has a relatively broad conception of cyber-security. It doesn't just aim to safeguard access and openness and to maintain reliability and interoperability, but also seeks the protection of fundamental rights, democracy and the rule of law in cyberspace. *"Cyberspace should be protected from incidents, malicious activities and misuse; and governments have a significant role in ensuring a free and safe cyberspace."* (European Commission, 2013) Wessel therefore rightly points out that there is criticism on the fact that the EU hasn't defined some key concepts closely related to cyber-security. These are cyber-resilience, cyber-defense, cyber-espionage and cyber-war.

One of the reasons for abandoning mere technical conceptions is the increase in scope of cybercrimes and its consequences. Earlier, I have already highlighted infrastructural impacts as a result of cyber-attacks. Criminals continue to have more and more sophisticated ways to commit crimes online. Examples are the emergence of 'ransom ware' and online identity fraud. They don't just penetrate systems and steal information, they use it to hold individuals, businesses, organizations and states hostage for ransom or other purposes. (United Nations, 2013) A common understanding on cyber-resilience *"…(adding the element of the ability of a system to recover from the effects of a security incident to full operational capacity)…"* (Wessel, 2015 (forthcoming)) is therefore essential.

The objects that the EU wants to protect range from citizens to Member States and the attacks that it wants to counter also range from individuals to foreign states. Cyber-defense covers the area *"…related to increasing the resilience of the communication and information systems supporting Member States' defence and national security interests…"* (Wessel, 2015 (forthcoming)) Accordingly, it is strange that the EU hasn't given a definition on this concept in the 2013 Strategy and neither in the accompanying Directive.

There is also online economic and inter-state espionage by state-sponsored groups. The United States and China have for example repeatedly accused each other of supporting cyber espionage on military, governmental and corporate targets. (Schwartz & Talley, 2015) The EU 2013 Strategy contains the following on cyber-espionage and although not mentioned as such, cyber-warfare: *"If the incident seems to relate to cyber espionage or a state-sponsored attack, or has national security implications, national security and defence authorities will alert their relevant counterparts, so that they know they are under attack and can defend themselves. Early warning mechanisms will then be activated and, if required, so will crisis management or other procedures. A particularly serious cyber incident or attack could constitute sufficient ground for a Member State to invoke the EU Solidarity Clause (Article 222 of the Treaty on the Functioning of the European Union)."* (European Commission, 2013) Whereas the consequences of cyber-espionage and 'serious attacks' are mentioned, they are not defined by the EU.

2.4 The United Nations

The difficulty for new initiatives to turn into concrete measures can also be observed at the UN. The United Nations have mostly treated cyber security issues in the General Assembly by using the Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security. Like most affairs, the UN tackles cyber security using a state-centered approach. The GGE's have produced yearly reports on cybercrime and related security issues. I will highlight some important reports and resolutions made by the General Assembly and analyze the UN's conception on cyber security.

In resolution 66/24 of 13 December 2011, the United Nations expressed concern over the possible misuse of 'technologies and means' resulting into destabilization of infrastructure of States and harm to security in civil and military fields. It also noted that it was imperative that information assets should not be used for criminal or terrorist schemes. The UN consequently asked its experts and Member States to research *"…existing and potential threats in the field of information security, as well as possible strategies to address the threats emerging in this field, consistent with the need to preserve the free flow of information."* (United Nations, 2011) Security measures were framed as 'cooperative measures' including norms, rules or principles of responsible behavior of States and confidence-building measures.

The GGE's created an important report in 2013. The report by the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security expanded on norms that should be followed in cyberspace. For the first time, they concluded that international law and norms under the UN Charter paradigm are applicable in this area including the norm of state responsibility for cyber-attacks originating from a states territory. In other words, they condemned wrongful acts committed by state proxies. Accordingly, international treaties such as the Universal Declaration of Human Rights containing respect for human rights and fundamental freedoms were deemed relevant for cyberspace. It also recognized that 'cooperative measures' can't be taken without the participation of the private sector and civil society due to the infrastructural cohesiveness of cyberspace itself and (social) consequences resulting from attacks. (United Nations, 2013)

Unfortunately, following this, the General Assembly adopted resolution 68/243 on 27 December 2013 which contents' were weaker than the GGE report. Although the GA only requested further research by the Secretary General and GGE's on the applicability of international rules of state responsibility, it did note the *"…importance of respect for human rights and fundamental freedoms in the use of information and communications technologies."* (United Nations, 2014)

So the UN uses a mostly state-centered approach to cyber security issues, though understanding the importance of cooperation with the private sector and civil society due to infrastructural cohesion in cyberspace and social consequences resulting from cyber-attacks. It also recognizes a large scope of cyber-attacks and deems online respect for human rights and fundamental freedoms as important. It perceives that there is no common understanding on the applicability of international norms such as of state behavior in cyberspace and calls for further research on this topic.

2.5 Conclusion

The second section of this paper explored what the EU's conception of cyber-security is and why it is tough for new legislative initiatives to take place.

Kruger concluded that the concept of cyber-security has remained mostly undefined and complicated. As Wessel sums it up, the broad scope of the area and fuzziness of the definitions make it more difficult for the EU to take new legislative initiatives. The broad scope of cyber-security is depicted by Nissenbaum. She showed a great contrast between 'technical computer security' and 'cyber-security'. The conception of cyber-security contains much more than technical computer security. Not only their scopes differ, but also social consequences, the target subjects and justifications.

The EU has defined the two concepts 'cyber-security' and 'cyber-crime' in its 2013 Strategy. Cyber-security is regarded as something that guards the cyber domain against threats, while cybercrime is a part of these threats originating from unlawful actions. The EU has a broad conception of cyber-security not only restricted to safeguarding access and openness and maintaining reliability and interoperability, but also protecting fundamental rights, democracy and the rule of law in cyberspace. Yet it has failed to clearly define key concepts closely related to cyber-security. These are cyber-resilience, cyber-defense, cyber-espionage and cyber-war.

The difficulty for new initiatives to turn into concrete measures can also be observed at the UN. The UN uses a mostly state-centered approach to cyber-security issues, though understanding the importance of cooperation with the private sector and civil society due to infrastructural cohesion in cyberspace and social consequences resulting from cyber-attacks. The GGE's concluded

in their 2013 Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security report that international law and norms under the UN Charter paradigm are applicable in this area including the norm of state responsibility for cyber-attacks originating from a states territory. Regrettably, the following resolution 68/243 by the General Assembly only called for further research on the applicability of international law and norms. It did recognize the large scope of cyber-attacks and deemed online respect for human rights and fundamental freedoms as important. These, however, are far from concrete measures.

3. EU cyber-security policy and regulation

The reason why it is difficult to create and enforce legislation in the area of cyber-security is not only caused by a broad scope of the concept and fuzzy definitions, but also by various institutional and competence problems of the EU.

3.1 Internal and external dimension of Union policy

The Union's policies have two dimensions: an internal one and external one. The internal dimension relates to the Internal Market and the Area of Freedom, Security and Justice (AFSJ), the external dimension to the foreign and security policy.

In order to understand how these are related, a closer look shall be taken at internal and external cyber-security policy and regulation in the EU. A short summary of the Pre-Lisbon situation shall be given, followed by a more comprehensive analysis of the Post-Lisbon status-quo. A clear difference in EU cyber-security policy and regulation pre- and post-Lisbon can be observed.

3.2 Pre-Lisbon

Policy coherence had always been problematic under the Pillar structure. (Carbone, 2008). This applied particularly on the area of cyber-security. As mentioned in the introductory section, policies on cyber-security issues were split between the three Pillars of the Union before 2009. These Pillars were: the European Communities (EC), Common Foreign and Security Policy (CFSP) and the Police and Judicial Co-operation in Criminal Matters (PJCC, now AFSJ). Under the Pillar structure, each contained different competences, responsibilities and decision making procedures.

In section 2 I argued that cyber-security is still mostly a broad, unclear concept which has evolved from a mere technical conception to one with broad social consequences. The challenges are abundant and diverse. Cyber-attacks vary in scope, can be on- and offline and can take place against individuals, businesses, organizations and even states. (United Nations, 2013) The problems created by cyber-attacks couldn't be solved by regulation from one pillar.

3.2.1 'Network and Information Security: Proposal for A European Policy Approach' (COM (2001) 298 final)

This was recognized by the Commission in the *'Network and Information Security: Proposal for A European Policy Approach'* (COM (2001) 298 final).

"Security is becoming a key priority because communication and information have become a key factor in economic and societal development. Networks and information systems are now supporting services and carrying data to an extent inconceivable only a few years ago. Their availability is critical for other infrastructures such as water and electricity supply. As everybody, business, private individuals, public administrations want to exploit the possibilities of communication networks, security of these systems is becoming a prerequisite for further progress." (Commission of the European Communities, 2001)

The Proposal recognized that the information society was growing at an alarming rate and that cyberspace would have an immense role in economic and social life. Therefore, Network and Information Security (NIS) was going to be crucial. The EU identified two main concerns: the increase of scope and damages caused by cyber-attacks and the fast speed technological developments.Due to abundant and diverse challenges, the Proposal attempted to create a more holistic NIS approach, with measures crossing pillars. These were:

"Awareness raising: A public information and education campaign should be launched and best practices should be promoted.

A European warning and information system: Member States should strengthen their Computer Emergency Response Teams (CERTs) and improve the co-ordination among them. The Commission will examine together with Member States how to best organise at European level data collection, analysis and planning of forward-looking responses to existing and emerging security threats.

Technology support: Support for research and development in security should be a key element in the 6th Framework Programme and be linked to the broader strategy for improved network and information security.

Support for market oriented standardisation and certification: European standardisation organisations are invited to accelerate work on interoperability; Commission will continue support for electronic signature and the further development of IPv6 and IPSec, Commission will assess the need for a legal initiative on the mutual recognition of certificates, Member States should review all relevant security standards.

Legal framework: The Commission will set up an inventory of national measures which have been taken in accordance with relevant Community law. Member States to support free circulation of encryption products. Commission will propose legislation on cybercrime.

Security in government use: Member States should incorporate effective an interoperable security solutions in their e-government and e-procurement activities. Member States should introduce electronic signatures when offering public services. The Commission will strengthen its security requirements in their information and communication system;

International co-operation: The Commission will reinforce the dialogue with international organisations and partners on network and information security." (Commission of the European Communities, 2001)

3.2.2 'A strategy for a Secure Information Society – "Dialogue, partnership and empowerment' (COM (2006) 251)

A second attempt on a holistic policy was: 'A strategy for a Secure Information Society – "Dialogue, partnership and empowerment' (COM (2006) 251). This strategy sought to 'revitalize' the 2001 Proposal.

"It reviews the current state of threats to the security of the Information Society and determines what additional steps should be taken to improve network and information security (NIS)." (Commission of the European Communities, 2006)

New concerns were identified and mentioned as such. Firstly, it identified a new type of cyber-criminals, who were more focused on using attacks to create profit rather than disruption. Examples of these new activities are illegal data mining, spam, spyware, phishing, other forms of malware and botnets. Secondly, new developments such as mobile devices, mobile networks and intelligent devices were rapidly growing thus posing new security challenges. Thirdly, by 2006, the rapid advancement resulted in cyberspace becoming *"…a core function of human social and economic interaction."* (Commission of the European Communities, 2006) Resilience became essential as critical infrastructures became more vulnerable because of interconnectivity. The public and private sectors still underestimated the security risks posed by these new challenges. For policy makers, the key challenge was *"…to achieve a holistic approach."* (Commission of the European Communities, 2006)

This Commission also perceived that they were heavily reliant on various private actors. Hence, a multi-stakeholder approach was developed.

"A secure Information Society must be based on enhanced NIS and a widespread culture of security. To this end, the European Commission proposes a dynamic and integrated approach that involves all stakeholders and is based on dialogue, partnership and empowerment. Given the complementary roles of public and private sectors in creating a culture of security, policy initiatives in this field must be based on an open and inclusive multi-stakeholder dialogue." (Commission of the European Communities, 2006)

3.2.3 Fragmentation and inefficiency

Yet, a single universal cyber-security policy was never fully realized. The proposals, although having cross-pillar elements, only contained CFSP affairs as far as disaster relief and crisis management. The main focus was on creating awareness and resilience of infrastructure in the private and public sectors, institutionalization and tackling cyber-crime. Furthermore, the 2006 strategy specifically mentioned that the key challenge was to achieve a holistic approach while mostly containing measures for the Internal Market.

Additionally, the Pillars produced an inefficient environment for the development of cyber-security policy. Disjunctive policies and strategies were made independently because Directorate-Generals (DG) of the Commission operated separately. For example, breaking into systems and stealing data is at first sight a criminal issue falling under the jurisdiction of the Third Pillar: Police and Judicial Co-operation in Criminal Matters reflected by *'the Proposal for a Council Framework Decision on attacks against information systems'* (COM (2002) 173 final). But what if the stolen data seriously affected the working of the internal market? Directive 2002/58/EC *'Concerning the processing of personal data and the protection of privacy in the electronic communications sector'* was respectively adopted under the First Pillar.

3.2.4 ENISA

Finally, the creation dedicated agencies who acted independent such as the European Network and Security Agency (ENISA) in 2004 made the matter even more complicated. ENISA was set up as a body of expertise (consisting out of stakeholders from: ICT professionals, academic expert, etc.). It *"…assists the European Commission in the technical preparatory work for updating and developing Community legislation in the field of Network and Information Security."* (ENISA, 2015)

3.3 Post-Lisbon

With the introduction of the Lisbon Treaty, the EU gained more legal coherence. Instead of competences existing in separate Pillars the EU became a single legal body based on the Treaty on the European Union (TEU) and the Treaty on the Functioning of the European Union (TFEU). The Charter of Fundamental Rights of the European Union also gained full legal effect. Decision making processes were streamlined by the introduction of the *'ordinary legislative procedure'*. (Best, 2008)

3.3.1 Absence in the Treaties

So the Lisbon Treaty vastly reformed the legal and institutional setup of the Union. The creation of the single legal body also linked internal and external policy as I will explain in the next section. Yet cyber-security, even though regarded as an important issue, was not specifically incorporated in the Treaties.

Indeed, *"While there seems consensus on the proliferation of incidents and risks related to cyber-security, one of the key problems underlying the EU initiatives is that 'cyber-security' as such is not mentioned as a theme – let alone a competence – in the EU Treaties."* (Wessel, 2015 (forthcoming))

3.3.2 'The Cyber-security Strategy of the EU: An Open, Safe and Secure Cyberspace' (JOIN (2013) 1 final)

Still, the elimination of the Pillar structure brought significant changes to the way EU institutions and agencies worked. Co-operation by DG's across Pillars was made possible and in the area of cyber-security this resulted into the joint 2020 strategy mentioned in Section 1 called *'the Cyber-security Strategy of the EU: An Open, Safe and Secure Cyberspace'* (JOIN (2013) 1 final). (European Commission, 2013) The joint strategy is an attempt *"…to mainstream cyberspace issues into EU external relations. When successful, this will allow the EU to link its internal policy initiatives and legislation to its external action, also in the area of foreign and security policy."* (Wessel, 2015 (forthcoming))

3.3.2.1 Challenges and principles

At this moment cyberspace takes an even more central role in our daily lives than with the previously discussed NIS Proposal in 2001 and SIS Strategy in 2006. Daily activity is heavily dependent on cyberspace. Governments have to safeguard access and openness and maintain reliability and interoperability and also protect fundamental rights, democracy and the rule of law. This has to be done while most of the internet is reliant on management by private actors. Cyberspace has many multi-level stakeholders in public and private spheres. In order for cyberspace to stay transparent, accountable and secure, principles were introduced in the joint strategy. These should guide policy of the EU and internationally and are as follows:

1. *"The EU's core values apply as much in the digital as in the physical world."* (European Commission, 2013)

2. *"Protecting fundamental rights, freedom of expression, personal data and privacy."* (European Commission, 2013)

3. *"Access for all."* (European Commission, 2013) Cyberspace is everywhere nowadays. Restrictions or limitations form a disadvantage to citizens.

4. *"Democratic and efficient multi-stakeholder governance."* (European Commission, 2013) As mentioned before, cyberspace has many actors in the public and private spheres. The involvement of all actors in management and development is required. Therefore the EU supports a multi-stakeholder governance approach.

5. *"A shared responsibility to ensure security."* (European Commission, 2013) Also, the many actors in this field require that all parties share responsibility. They don't just have to take care of themselves, but also cooperate if the situation calls for it.

3.3.2.2 Objectives

Accordingly, the new unified strategy contained five 'strategic priorities' with elements from the Internal Market, AFSJ and CFSP:

"The strategy articulates the EU's vision of cyber-security in terms of five priorities:

1. Achieving cyber resilience,

2. Drastically reducing cybercrime,

3. Developing cyber defence policy and capabilities related to the Common Security and Defence Policy (CSDP),

4. Developing the industrial and technological resources for cyber-security,

5. Establishing a coherent international cyberspace policy for the European Union and promoting core EU values." (European Commission, 2013)

3.3.2.3 Measures

In the Strategy, the Commission has made a division of responsibilities between itself, other EU institutions, EU agencies, Member States and the private sector.

To achieve the objective of improving cyber-resilience, the Commission continued to identify and develop resilience for vulnerable critical infrastructure. They also launched the project CIP-ICT PSP-2012-6, 325188 to counter botnets and malware. This project was a 'framework for coordination and cooperation' between Member States and the private sector. ENISA was charged with increasing its expertise on security and resilience of critical infrastructures, the investigation of the usefulness of security response teams and international and European cyber-security exercises. The Parliament and Council were invited to adopt the 2013 NIS Proposal (this Proposal will be discussed in the next section). The private sector was asked to establish best practices, promote information sharing and invest in cyber-security. In accordance with historical developments, awareness campaigns again had an important role in the Strategy. ENISA was asked to support the Commission in the creation of NIS 'cyber-security championships' for university students. It was also asked to develop a voluntary certification program for professionals on NIS. The organization of a 'cyber-security month' was asked of Member States together with the private sector and the United States. MS were also asked to improve NIS education and training initiatives. The private parties were asked to broadly promote awareness, especially accountability of executives.

To tackle cybercrime, the EU calls upon the rapid adoption of strong and effective legislation. This can be achieved by ratifying the 'Budapest Convention' made by the Council of Europe. (Council of Europe, 2001) This Convention contained substantive cybercrime law for states to implement. As of now, Greece and Ireland are the only EU Member States who done so. Furthermore the swift development of cybercrime tools requires Member States to improve their operational capability. Cooperation with the European Cybercrime Centre (EC3) of Europol can be used to identify the best operational practices. Moreover, Member States have to improve coordination among themselves, with the private sector and with other states outside the EU. An example of this global multi-level coordination is given in the form of the 'Global Alliance against Child Sexual Abuse Online' (European Commission, 2012). Other agencies such as the European Police College (CEPOL) and Eurojust were asked to work together in order to identify potential barriers for more cooperation, to improve the expertise of law enforcement and to increase the effectiveness of their existing mandates and competences.

On CFSP/CSDP issues, the focus lies on increasing the resilience of governmental, defense and other critical infrastructure, on cyber-defense only coordinating and supporting measures are mentioned:

"The High Representative will focus on the following key activities and invite the Member States and the European Defence Agency to collaborate:

Assess operational EU cyberdefence requirements and promote the development of EU cyberdefence capabilities and technologies to address all aspects of capability development - including doctrine,

leadership, organisation, personnel, training, technology, infrastructure, logistics and interoperability;

Develop the EU cyberdefence policy framework to protect networks within CSDP missions and operations, including dynamic risk management, improved threat analysis and information sharing. Improve Cyber Defence Training & Exercise Opportunities for the military in the European and multinational context including the integration of Cyber Defence elements in existing exercise catalogues;

Promote dialogue and coordination between civilian and military actors in the EU – with particular emphasis on the exchange of good practices, information exchange and early warning, incident response, risk assessment, awareness raising and establishing cybersecurity as a priority

Ensure dialogue with international partners, including NATO, other international organisations and multinational Centres of Excellence, to ensure effective defence capabilities, identify areas for cooperation and avoid duplication of efforts." (European Commission, 2013)

The fourth priority is focused on Research & Development and innovation: the reduction of reliance on foreign technology by MS, the creation of cyber-security instruments and harmonization for metrics for appraising risk premiums.

The last measure is focused on establishing external cyber-security policy for the Union in order to promote its core values. A coherent policy should be developed by the Commission, High Representative and the Member States. Problems should be tackled by using the CFSP framework. *"To address global challenges in cyberspace, the EU will seek closer cooperation with organisations that are active in this field such as the Council of Europe, OECD, UN, OSCE, NATO, AU, ASEAN and OAS. At bilateral level, cooperation with the United States is particularly important and will be further developed, notably in the context of the EU-US Working Group on Cyber-Security and Cyber-Crime."* (European Commission, 2013) Not only cooperation with these organisations is required, but also cooperation with third countries. The EU seeks to create an area of freedom and fundamental rights in cyberspace, advance democracy and to enforce the legal obligations established in the EU Charter of Fundamental Rights, the European Convention on Human Rights and the International Covenant on Civil and Political Rights. The EU does not want to create new international legal instruments. On armed conflicts, the EU deems International Humanitarian Law and Human Rights Law to be applicable.

3.3.4 Internal dimension

As mentioned before, the EU's internal dimension exists out of the Internal Market (former Pillar 1) and the AFSJ (former Pillar 3). With the introduction of the Lisbon Treaty, the EU now had a solid legal basis for both areas. I will first discuss the Internal Market, these competences were mostly, already existent in the Pre-Lisbon situation. Post-Lisbon, the AFSJ gained significantly more tools for EU actions.

3.3.4.1 Cyber-security competences for the Internal Market

The legal basis for cyber-security policy making in the Internal Market was explained in the 2013 Directive Proposal (COM (2013) 48 final). This Directive was the main action of the Cyber Security Strategy discussed in section 3.3.2. (European Commission, 2013) The Directive's subject matter is mentioned in Article 1. It is to lay *"…down measures to ensure a high common level of network and information security (hereinafter referred to as "NIS") within the Union."* (European Commission, 2013) I won't specifically explore every single provision in the Directive. It generally contained Internal Market provisions for measures, mentioned in the 2013 Strategy. The most relevant part for

this paper, is the legal basis which the Directive is based on and where its competences come from. This will be discussed in the next part.

3.3.4.2 'Proposal for a Directive of the European Parliament and of the Council - concerning measures to ensure a high common level of network and information security across the Union' (COM (2013) 48 final)

The legal basis of the Proposal was based on Articles 26 and 114 TFEU.

Article 26 TFEU (ex. Article 14 TEC): *"1. The Union shall adopt measures with the aim of establishing or ensuring the functioning of the internal market, in accordance with the relevant provisions of the Treaties.*

2. The internal market shall comprise an area without internal frontiers in which the free movement of goods, persons, services and capital is ensured in accordance with the provisions of the Treaties.

3. The Council, on a proposal from the Commission, shall determine the guidelines and conditions necessary to ensure balanced progress in all the sectors concerned." (European Union, 2012)

Article 114 TFEU (ex. Article 95 TEC): *"1. Save where otherwise provided in the Treaties, the following provisions shall apply for the achievement of the objectives set out in Article 26. The European Parliament and the Council shall, acting in accordance with the ordinary legislative procedure and after consulting the Economic and Social Committee, adopt the measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have as their object the establishment and functioning of the internal market…"* (European Union, 2012)

These Articles already provided competence for Internal Market cyber-security actions Pre-Lisbon. As mentioned in the 2013 Strategy, secure NIS are critical for economic activity and growth. The nature of cyberspace makes these systems interwoven and not restricted to territorial borders. The large scope and interconnectivity make small disturbances having huge consequences. In other words, the Internal Market of the Union needs stable, resilient and operational NIS. For instance, Regulation EC/460/2004 based on (now) Article 114 TFEU was used to create ENISA in order to achieve harmonization of NIS rules in the Internal Market. Divergent NIS rules in Member States form an obstacle for the Internal Market. Therefore, cyber-security policy can be made by the EU using Internal Market competences.

3.3.4.3 Subsidiarity and proportionality

Obviously, EU action in this area has to abide by the principles of subsidiarity and proportionality laid down in Article 5 TEU.

The Directive gives the following reasons for why the subsidiarity principle is sustained. Firstly, without EU level intervention, Member States would act alone without regard to the interconnectivity of cross-border NIS systems. Secondly, non-binding instruments have only achieved cooperation among a small amount of MS who have a high level of capabilities. A level playing field can only be established by introducing regulatory obligations at the EU level. EU wide regulations would increase the performance of national policies by introducing minimum NIS standards.

The proportionality of the measures can also be justified. Firstly, the proposed actions are only minimum requirements. Member States will have the further freedom to consider specific national needs (Article 2: *"Member States shall not be prevented from adopting or maintaining provisions ensuring a higher level of security, without prejudice to their obligations under Union law"*

(European Commission, 2013)). Secondly, the provision regarding risk management only applies to critical entities. The proposed measures are also equivalent to the hazards. Thirdly, the reporting of NIS incidents only concerns the most serious ones. Finally, the costs to fund these measures will not be out of proportion, because current rules already cover a lot.

In short, the Directive states that the EU is better suited to achieve the objectives: *"…the EU may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality, the proposed Directive does not go beyond what is necessary in order to achieve those objectives."* (European Commission, 2013)

3.3.4.4 Sanctions

What is interesting is that Article 17 of the Directive proposal states that Member States should implement a sanctioning system for *"… infringements of the national provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented. The sanctions provided for must be effective, proportionate and dissuasive..."* (European Commission, 2013) Yet, it does not say how these sanctions should look like.

3.3.4.5 Enforcement in the Internal Market

Article 258 (ex Article 226 TEC): *"If the Commission considers that a Member State has failed to fulfil an obligation under the Treaties, it shall deliver a reasoned opinion on the matter after giving the State concerned the opportunity to submit its observations."* (European Union, 2012)

By basing the cyber-security policy on the Internal Market competence, the infringement laid down in Article 258 TFEU is usable. If MS fail to comply, the Commission may start a procedure. This is an important enforcement tool. For the Internal Market, this procedure had been available Pre-Lisbon. For the AFSJ, the ability to enforce expanded its possibilities greatly.

3.3.4.6 Cyber-security competences for the Area of Freedom, Security and Justice

The abolishment of the Pillar structure brought the AFSJ matters partly under supranational competences. The functioning was previously based on intergovernmental cooperation with little input from EU organs such as the Commission, Parliament and Court of Justice.

This is illustrated by the following: the AFSJ now contains the term 'computer crime' in **Article 83 TFEU (ex. Article 31 TEU):** *"1. The European Parliament and the Council may, by means of directives adopted in accordance with the ordinary legislative procedure, establish minimum rules concerning the definition of criminal offences and sanctions in the areas of particularly serious crime with a cross-border dimension resulting from the nature or impact of such offences or from a special need to combat them on a common basis.*

These areas of crime are the following: terrorism, trafficking in human beings and sexual exploitation of women and children, illicit drug trafficking, illicit arms trafficking, money laundering, corruption, counterfeiting of means of payment, ***computer crime*** *and organised crime.*

On the basis of developments in crime, the Council may adopt a decision identifying other areas of crime that meet the criteria specified in this paragraph. It shall act unanimously after obtaining the consent of the European Parliament.

2. If the approximation of criminal laws and regulations of the Member States proves essential to ensure the effective implementation of a Union policy in an area which has been subject to harmonisation measures, directives may establish minimum rules with regard to the definition of criminal offences and sanctions in the area concerned. Such directives shall be adopted by the same

ordinary or special legislative procedure as was followed for the adoption of the harmonisation measures in question, without prejudice to Article 76." (European Union, 2012)

With cybercrime now mentioned in this Article of the Treaty, the EU gained the powers to *"…establish minimum rules with regard to the definition of criminal offences and sanctions in the area concerned…"* (European Union, 2012) Also, the Commission can now launch initiatives in this area using the ordinary or special legislative procedures.

The previously mentioned permanent Computer Emergency Response Team (CERT-EU) was created in 2012. Direct support of the European Cybercrime Centre (EC3) of Europol by the Commission was also made possible, because of the possibility to take initiatives.

3.3.4.7 Enforcement in the AFSJ

Along with the ability to create EU legislation, came the ability for enforcement. Unlike the Internal Market, the EU previously did not have the ability to administer punishment to dissent Member States. Correspondingly, the ECJ gained jurisdiction over AFSJ matters. This greatly enhanced the capability of the Union to combat cyber-crime.

However, Article 276 TFEU was also introduced providing some restrictions to the ECJ's jurisdiction. It will not have jurisdiction in AFSJ matters *"…with regard to the maintenance of law and order and the safeguarding of internal security."* (European Union, 2012)

Article 276 TFEU: *"In exercising its powers regarding the provisions of Chapters 4 and 5 of Title V of Part Three relating to the area of freedom, security and justice, the Court of Justice of the European Union shall have no jurisdiction to review the validity or proportionality of operations carried out by the police or other law-enforcement services of a Member State or the exercise of the responsibilities incumbent upon Member States with regard to the maintenance of law and order and the safeguarding of internal security."* (European Union, 2012)

3.3.5 External dimension

Regarding external policy, the scope of the High Representative of the Union for Foreign Affairs and Security Policy (HR) was increased, a new European External Action Service (EEAS) was established to accomplish Common Foreign and Security Policy (CFSP) and Common Security and Defense Policy (CSDP) objectives and the European Defense Agency (EDA) were formally brought under the HR.

The CFSP was mainly created in order to organize the EU's security, defence and other related diplomacy actions and has come into existence as a compromise between the EU's ambition to have a common foreign policy and the Member States' desire for intergovernmental cooperation on this matter. Member States have always been reluctant to hand over powers in this policy field. More integration was rejected when the Constitutional Treaty failed in 2003. *"A consequence of this is precisely the vague, ill-defined and complex nature of the EU's competence in foreign and international security policy following the coming into force of the Treaty of Lisbon."* (Dewar, 2015)

The CFSP is a high level policy area in the EU due to the sensitivity of the issues and the importance of the actors involved. Decisions in the CFSP are taken by unanimity of the European Council or Council of Ministers on proposal by the HR and can be categorized in four types: on strategic and objectives, on common positions, on joint action and on implementing arrangements.

The new strategy: *'the Cybersecurity Strategy of the EU: An Open, Safe and Secure Cyberspace',* for the first time, linked cyber-security to national security actions set out in the CSDP. The incorporation of CFSP issues in the cyber-strategy reflect the new uniform policy creating possibilities made possible by the Lisbon Treaty.

3.3.5.1 Questions of competence

Article 24(1) TEU (ex. Article 11 TEU): *"The Union's competence in matters of common foreign and security policy shall cover all areas of foreign policy and all questions relating to the Union's security, including the progressive framing of a common defence policy that might lead to a common defence.*

The common foreign and security policy is subject to specific rules and procedures. It shall be defined and implemented by the European Council and the Council acting unanimously, except where the Treaties provide otherwise. The adoption of legislative acts shall be excluded…" (European Union, 2012)

Article 26(1) TEU (ex. Article 13 TEU): *"The European Council shall identify the Union's strategic interests, determine the objectives of and define general guidelines for the common foreign and security policy, including for matters with defence implications. It shall adopt the necessary decisions…"* (European Union, 2012)

Article 42(1) TEU (ex. Article 17 TEU): *"The common security and defence policy shall be an integral part of the common foreign and security policy. It shall provide the Union with an operational capacity drawing on civilian and military assets. The Union may use them on missions outside the Union for peace-keeping, conflict prevention and strengthening international security in accordance with the principles of the United Nations Charter. The performance of these tasks shall be undertaken using capabilities provided by the Member States."*

The legal basis of the CFSP and CSDP can be found in Chapter 2 TEU and more specifically in the above articles. Even though foreign and security policy has a base in the Treaties, both suffer from the same problem. These are questions of competence.

Firstly, the nature of the competence of the CFSP itself is unclear. Articles 3, 4, 5 and 6 TFEU mentions the categories of competence of the EU. These are: exclusive competences, shared competences and supporting, coordinating and supplementing competences. The CFSP is not listed here. Although not mentioned as such in the Treaties, the CFSP has in reality remained a de facto *'separate pillar'* in the Post-Lisbon EU. (Wouters, Coppens, & Meester, 2008) (Nugent & Rhinard, 2011) Specific legislative and implementation procedures still persist in this area. For instance, CFSP matters are adopted by decision and require unanimity of the Council. Articles 24 and 36 TEU restrict the application of EU legislative procedures and the Parliament's role is also merely consulting. The Commission also has a different, more limited role compared to the ordinary legislative procedure. It can't take the initiative in these matters. The limitation of supranational procedures in the CFSP is also illustrated by the fact that the flexibility clause, Article 352 TFEU is excluded from*"…attaining objectives pertaining to the common foreign and security policy…"* (European Union, 2012)

3.3.5.2 No enforcement for the CFSP

In contrast to Post-Lisbon internal policy, the ECJ's jurisdiction does not extend to the CFSP. Article 275 TFEU clearly states this. The ECJ only has the ability to review the legality of decisions providing for restrictive measures against natural or legal persons.

Article 275 TFEU: *"The Court of Justice of the European Union shall not have jurisdiction with respect to the provisions relating to the common foreign and security policy nor with respect to acts adopted on the basis of those provisions.*

However, the Court shall have jurisdiction to monitor compliance with Article 40 of the Treaty on European Union and to rule on proceedings, brought in accordance with the conditions laid down in the fourth paragraph of Article 263 of this Treaty, reviewing the legality of decisions providing for

restrictive measures against natural or legal persons adopted by the Council on the basis of Chapter 2 of Title V of the Treaty on European Union." (European Union, 2012)

So even though CFSP issues are included in the cyber strategy, the EU has in fact no supranational way to create and enforce legislation in this area. The processes remains largely inter-governmental and separated from the other EU objectives. This is illustrated by the following: *"In most cases CFSP Decisions are adopted without any debate in the Council; they have been prepared by the Council's subsidiary organs and a consensus has already been established between the representatives of the Ministers for Foreign Affairs on the basis of prepatory work by the various subsidiary organs of the Council."* (Wessel, 2015 (forthcoming))

3.3.5.3 Limited mandate CSDP

Also, the use of military force under the CSDP is mostly limited to the 'Petersberg Tasks'. These are listed in Article 42(1) TEU: Humanitarian and rescue, peacekeeping, combat forces in crisis management including peacemaking. (European Union, 2012)

Other tasks are mentioned in Article 43(1) TEU: joint disarmament, military advice and assistance tasks, post-conflict stabilization and anti-terrorism. (European Union, 2012) The nature of these tasks are in strong contrast to the challenges that international cyber-defense pose.

For instance, it is a fact that current and previous operations under the CSDP flag take place in multiple continents. Yet, they are restricted to one or at most several bordering states and its waters at once. (EEAS, 2015) Cyber-attacks don't come from one and cyber-defense is neither restricted to one geographical region. Attacks can be initiated by anyone, anywhere.

In most cases the search for a perpetrator leads to a futile quest (Broadhurst, 2006), but what if the perpetrator is identified as a state or state-sponsored group? Does a cyber-attack satisfy the conditions for an armed attack? Perhaps. (Tsagourias, 2012) As Wessel points out, the European Parliament has mentioned *"…cyberattacks as a reason to invoke the so-called 'mutual defence clause'…"* (Wessel, 2015 (forthcoming)) The clause is incorporated as Article 42(7) TEU and is applicable if a cyber-attack causes a Member States' security to be significantly threatened by its consequences.

Article 42(7) TEU: *"If a Member State is the victim of armed aggression on its territory, the other Member States shall have towards it an obligation of aid and assistance by all the means in their power, in accordance with Article 51 of the United Nations Charter. This shall not prejudice the specific character of the security and defence policy of certain Member States.*

Commitments and cooperation in this area shall be consistent with commitments under the North Atlantic Treaty Organisation, which, for those States which are members of it, remains the foundation of their collective defence and the forum for its implementation."

If the clause is triggered, cyber-defense becomes a military issue. The Treaty specifically refers to NATO in Article 42(2) TEU when military attacks arise.

Article 42(2) TEU: *"…The policy of the Union in accordance with this Section shall not prejudice the specific character of the security and defence policy of certain Member States and shall respect the obligations of certain Member States, which see their common defence realised in the North Atlantic Treaty Organisation (NATO), under the North Atlantic Treaty and be compatible with the common security and defence policy established within that framework."* (European Union, 2012)

In short, in this case, competence will no longer lie with the CFSP (or EU in that matter) but instead a Member States' own and probably also a North Atlantic Treaty Organization (NATO) problem.

Particularly problematic will be if a Member State becomes the victim of a terrorist attack or if the attack has disastrous consequences. In that case, the Parliament has decided that Article 222 TFEU,the solidarity clause, could possibly be triggered.

Article 222 TFEU: *"The Union and its Member States shall act jointly in a spirit of solidarity if a Member State is the object of a terrorist attack or the victim of a natural or man-made disaster. The Union shall mobilise all the instruments at its disposal, including the military resources made available by the Member States,…"* (European Union, 2012)

On the other hand, *"…invoking a solidarity or a mutual defence clause will most probably be driven more by political incentives than by legal doctrinal analysis."* (Wessel, Towards EU Cybersecurity Law: Regulating a New Policy Field, 2015 (forthcoming))

3.4 Conclusion

The second section contained the cyber-security policies and the way they were regulated Pre-Lisbon and Post-Lisbon. The reason why it is difficult to create and enforce legislation in the area of cyber-security is not only caused by a broad scope of the concept and fuzzy definitions, but also by various institutional and competence problems of the EU.

Before the ratification of the Lisbon Treaty, policy coherence was a widespread problem throughout the Union, especially on the area of cyber-security. Attempts at creating a holistic approach were made. The 2001 NIS Proposal and the 2006 SIS Strategy were not fully uniform, with Pillar 2 affairs limited to disaster relief and crisis management. Additionally, fragmentation caused policies and strategies to be developed independently. DGs of the Commission belonging to different pillars operated separately.

Post-Lisbon, the EU became a single legal body by formally abolishing the Pillar structure and thus gained more coherence. Co-operation by DG's across Pillars became possible and for the first time the area of cyber-security had a unified strategy containing Internal Market, CFSP and AFSJ elements presented in 2013: *'the Cybersecurity Strategy of the EU: An Open, Safe and Secure Cyberspace'* (European Union, 2012) However, cyber-security was still not mentioned as a theme or competence in the Treaties.

Internally, the EU now had a solid legal basis for former EC and PJCC policy making. Cyber-security competence in the Internal Market remained unchanged compared to the Pre-Lisbon situation. Its basis lies in Articles 26 and 114 TFEU and enforcement was already possible.

For the AFSJ, the abolishment of the pillar structure brought it under supranational competence. Computer crime was included in Article 83 TFEU and AFSJ matters could now be initiated and enforced by the Union. This led to the establishment of the CERT-EU and support of Europol's EC3 by the Commission. The EU, according to Article 276 TFEU, however, still has no possible to enforce matters with regard to the maintenance of law and order and the safeguarding of internal security.

Externally, the EEAS was established, the scope of the HR was increased and the CFSP, CSDP and EDA were brought under their umbrella. The creation of the holistic cyber-security strategy was unique and progressive, reflecting the new possibilities made possible by the Lisbon Treaty. Yet it raised the same questions of competence where the CFSP suffered from.

The CFSP and CSDP have their legal basis in Articles 24, 26 and 42 TEU. Despite them being mentioned in the Treaties, the nature of the competence is still unclear: the CFSP is not listed in Articles 3, 4, 5 and 6 TFEU as a category of competence. It has also remained a de facto *'separate pillar'* with intergovernmental characteristics in the Post-Lisbon EU. Specific legislative and implementation procedures limited the Parliament's and Commission's role. Furthermore, according to Article 275 TFEU, the ECJ does not have jurisdiction in the context of the CFSP. In other words: the EU has in fact no supranational way to create and enforce legislation in this area.

Secondly, the CSDP has a limited mandate. The use of military force under the CSDP is mostly restricted to the so-called 'Petersberg Tasks': humanitarian and rescue, peacekeeping, combat forces in crisis management, including peacemaking plus joint disarmament operations, military advice and assistance and post-conflict stabilization. These tasks are fundamentally different to the challenges that international cyber-defense pose. Cyber-attacks can be initiated by anyone, anywhere and are not restricted to a geographical region.

It is hard albeit impossible to identify cyber-criminals accurately. In most cases this is resource and time intensive - and in the end - futile quest. Likewise, if the perpetrator is a state or state-sponsored group it might qualify as an armed attack. Consequently Article 42 TEU specifically removes the EU's qualification to deal with the problem and instead defers it to Member States themselves and probably NATO as well. Moreover, the solidarity clause in Article 222 TFEU adds an extra dimension in case of a terrorist attack and disaster.

4. The optimal use of competences by the EU

4.1 Interwoven nature of cyberspace

The greatest reasons for a holistic EU approach and also the greatest pitfalls are the large scope, cross-border element and interwoven nature of cyberspace. Cyber-security, as we have seen has a large scope covering many areas. Moreover, there are no clear borders in cyberspace.

It seems obvious that the EU as a supranational actor should regulate this field. In the Cyber Security Strategy 2013, the EU attempts to mainstream cyberspace matters into external relations. *"When successful, this will allow the EU to link its internal policy initiatives and legislation to its external action, also in the area of foreign and security policy."* (Wessel, 2015 (forthcoming))

Yet, for holistic cyber-security initiatives to succeed, strong inter-institutional cooperation is required. (Wessel, 2015 (forthcoming)) This strong inter-institutional cooperation is not possible within the current EU framework. While the EU abolished the pillars in the Lisbon Treaty, different modi operandi still persist within this single structure. (Bickerton, Hodson, & Puetter, 2015) All EU action has to be based on Treaty provisions or formal EU legislation. Competences are also restricted to their own policy area. This is the principle of conferral. Each area, as we have seen, has its own set of rules.

Correspondingly, policy makers have to choose a specific legal basis for their initiatives. The different modi operandi have as a consequence that the choice of legal basis has a huge impact. It directly affects the powers the various EU institutions and influence of Member States. While internal procedures are leaning more towards the supranational, external foreign and security competences have mostly remained with the Member States themselves. In practice, it is hard to separate internal and external dimensions. (Wessel, 2015 (forthcoming)) Conflicts rise due to the differences in modi operandi. In the worst case, groups of Member States will operate on an intergovernmental basis, outside the EU Treaty framework. (Bickerton, Hodson, & Puetter, 2015)

In addition, an effective response against cyber-attacks *"…requires cross-border cooperation between authorities. It is here that the current division of responsibilities between civil defence, military defence, and law enforcement falters."* (Benediek & Porter in (Wessel, 2015 (forthcoming))

4.1.1 Opt-outs

Moreover, the EU has a tendency for 'differentiated integration'. This is illustrated by the various opt-outs. Currently, four Member States have opt-outs from EU provisions. Denmark, Poland, Ireland and the United Kingdom.

Ireland and the United Kingdom have opted out the Schengen Agreement. Denmark and the United Kingdom opted-out the Economic and Monetary Union. (Peers, 2011)

Denmark has an opt-out on defense components of Treaties, the CSDP. At the entry of the Lisbon Treaty, Poland and the United Kingdom have made efforts for an opt-out on the EU Charter of Fundamental Rights. This resulted in Protocol 7 of the Charter. Yet, it was shown that the Charter has legal force in the two Member States, despite this Protocol. (House of Commons, 2013) Denmark, Ireland and United Kingdom have partial opt-outs of the AFSJ. Ireland and the UK can do this on a case-by-case basis, while Denmark has a more rigid opt-out clause. (Peers, 2011)

Differentiated integration is not desirable for cyber-security policies. As noted in the previous section, we need strong cooperation in this field.

4.2 External competences

The EU seeks to link internal and external policy with each other in the field of cyber-security. As demonstrated, the internal mechanisms are relatively solid compared to the external ones. I will argue that the current external CFSP/CSDP legal basis is unsuited for the creation of cyber-security policy.

4.2.1 Questions of competence and weak external action

The external Union competences are surrounded by many questions. This has been discussed in section 3.3.5. The absence of judicial review along with the different modi operandi offers an explanation for not realizing an integrated security policy. The 2013 Cyber Security Strategy acknowledges that cyber-defense is a dimension of cyber-security, but only contains coordination and dialogue actions for the EU and NATO. (Wessel, 2015 (forthcoming)) So even if external action is mainstreamed into the Strategy, strong and effective EU-level measures can't be realized due to legal and institutional weaknesses.

4.2.2 Multi-level stakeholders

Besides questions of competence, external policy making has another problem. The creation of cyber-security involves many actors in the public and private spheres. Private actors are heavily involved in the day-to-day managing and operating of cyberspace and thus pivotal for securing it. External action in the context of the CFSP/CSDP, due to the actors involved and its unique decision making process, takes the process towards 'high politics' without private involvement in the process.

4.3 Consistency

Article 13 TEU: *"The Union shall have an institutional framework which shall aim to promote its values, advance its objectives, serve its interests, those of its citizens and those of the Member States, and ensure the consistency, effectiveness and continuity of its policies and actions…"* (European Union, 2012)

Article 21 TEU: *"…The Union shall ensure consistency between the different areas of its external action and between these and its other policies. The Council and the Commission, assisted by the High Representative of the Union for Foreign Affairs and Security Policy, shall ensure that consistency and shall cooperate to that effect."*

These two articles contain the Union's obligation to create coherent, consistent and effective policy. Due to the previously discussed problems rising because of the broad scope of cyber-security, it is highly doubtful that the EU will meet these principles when creating policy in this area.

Indeed, *"While the new treaty rules may provide some indication of the correct legal basis, the wide variation in cybersecurity measures will continue to form an obstacle on the route to a comprehensive and consistent policy in that area."* (Wessel, 2015 (forthcoming))

4.4 Main Conclusion

Competences of the EU for the creation of internal (cyber-security) policy are relatively solid compared to external policy under the Post-Lisbon regime. The EU created and enforced legislation for the Internal Market and AFSJ issues. Yet, in my opinion, the optimal use of competence for the EU in its current framework, is a coordinating and supporting role in the policy area of cyber-security. It should not seek to create a set rules, because internal and external policy in this field are hard to separate. Also, referring to section 1, many terms related to cyber-security have not been defined by the EU. At least, without the EU further consolidating by making fundamental changes, uniform cyber-security regulation will make matters more complicated, inconsistent and unclear.

Bibliography

Best, E. (2008). The Lisbon Treaty: A Qualified Advance for EU Decision-Making and Governance. *EIPAScope*, 1-6. Retrieved from http://aei.pitt.edu/11041/1/20080509183728_SCOPE2008-1-2_EdwardBest.pdf

Bickerton, C. J., Hodson, D., & Puetter, U. (2015). *The New Intergovernmentalism States and Supranational Actors in the Post-Maastricht Era.* Oxford: Oxford University Press.

Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. *International Journal of Police Strategies & Management*, 408-433. Retrieved from http://www.emeraldinsight.com/doi/full/10.1108/13639510610684674

Brown, I. (2011). Reducing Systemic Cybersecurity Risk. *Organisation for Economic Cooperation and Development Working Paper No. IFP/WKP/FGS(2011)3*, January.

Bunker, G. (2013, February 13). *Cyber security for the EU: from strategy to successful deployment*. Retrieved from The Guardian: http://www.theguardian.com/media-network/media-network-blog/2013/feb/13/eu-cyber-security

Carbone, M. (2008). Mission Impossible: the European Union and Policy Coherence for Development. *Journal of European Integration*, 323-342. Retrieved from http://www.tandfonline.com/doi/abs/10.1080/07036330802144992#.Vb5npG6qpBc

Commission of the European Communities. (2001, June 6). *COMMUNICATION FROM THE COMMISSION TO THE COUNCIL, THE EUROPEAN PARLIAMENT, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS - Network and Information Security: Proposal for A European Policy Approach (COM (2001) 298 final).* Retrieved from https://ccdcoe.org/sites/default/files/documents/EU-010606-NISProposal.pdf

Commission of the European Communities. (2006). *COMMUNICATION FROM THE COMMISSION TO THE COUNCIL, THE EUROPEAN PARLIAMENT, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS - A strategy for a Secure Information Society – "Dialogue, partnership and empowerment" (COM (2006) 251).* Retrieved from http://ec.europa.eu/information_society/doc/com2006251.pdf

Council of Europe. (2001, November 23). *Convention on Cybercrime.* Retrieved from Council of Europe: http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm

Dewar, R. (2015). *Cyber-Lisbon? The Impact of the Treaty of Lisbon on European Union Cybersecurity Policy.* Retrieved from European Union Studies Association: https://eustudies.org/conference/papers/download/107

EEAS. (2015). *About CSDP - The Petersberg Tasks*. Retrieved from European External Action Service: http://eeas.europa.eu/csdp/about-csdp/petersberg/index_en.htm

EEAS. (2015, June). *Ongoing missions and operations*. Retrieved from European External Action Service: http://eeas.europa.eu/csdp/missions-and-operations/index_en.htm

Eneken, T. (2011). Ten Rules for Cyber Security. *Survival: Global Politics and Strategy*, 119-132.

ENISA. (2015). *About ENISA*. Retrieved from European Union Agency for Network and Information Security: http://www.enisa.europa.eu/about-enisa

European Commission. (2012, November 30). *Combating sexual abuse of children online: a Global Alliance for greater results.* Retrieved from European Commission - Migration and Home Affairs: http://ec.europa.eu/dgs/home-affairs/what-is-new/news/news/2012/20121130_02_en.htm#/c

European Commission. (2013). *EU Cybersecurity plan to protect open internet and online freedom and opportunity.* Retrieved from https://www.ncsc.nl/binaries/content/documents/ncsc-en/current-topics/news/eu-launches-cyber-security-strategy/1/EU%2Bstrategy%2Bpress%2Brelease.pdf

European Commission. (2013, February 7). *EU Cybersecurity plan to protect open internet and online freedom and opportunity - Cyber Security strategy and Proposal for a Directive.* Retrieved April 21, 2015, from European Commission: http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

European Union. (2007). *Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community.* Retrieved from EUR-Lex: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:C:2007:306:FULL&from=EN

European Union. (2012, October 26). *Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union.* Retrieved from EUR-Lex: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:12012M/TXT

European Union. (2015). *The principle of subsidiarity*. Retrieved from EUR-Lex: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:ai0017

Hansen, L., & Nissenbaum, H. (2009, December). Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly*, 1155-1175. Retrieved from http://onlinelibrary.wiley.com/doi/10.1111/j.1468-2478.2009.00572.x/full

House of Commons. (2013). *The application of the EU Charter of Fundamental Rights in the UK: a state of confusion.* European Scrutiny Committee. Retrieved from http://www.publications.parliament.uk/pa/cm201314/cmselect/cmeuleg/979/979.pdf

Irion, K. (2013). The Governance of Network and Information Security in the European Union: The European Public-Private Partnership for Resilience (EP3R). In J. Kruger, B. Nickotay, & S. Gaycken, *The Secure Information Society* (pp. 83-116). London: Springer.

Kruger, D. (2014). Radically Simplifying Cyber Security. In S. Suh, J. Tanik, J. Carbone, & A. Eroglu, *Applied Cyber-Physical Systems* (pp. 51-61). New York: Springer.

Luiijf, E., Besseling, K., & de Graaf, P. (2013). Nineteen national cyber security strategies. *International Journal of Critical Infrastructures*, 3-31. Retrieved from http://www.inderscienceonline.com/doi/abs/10.1504/IJCIS.2013.051608

Nissenbaum, H. (2005, June). Where Computer Security Meets National Security. *Ethics and Information Technology*, 61-73. Retrieved from http://link.springer.com/article/10.1007%2Fs10676-005-4582-3

Nugent, N., & Rhinard, M. (2011). The European Commission and the European Union's External Relations after the Lisbon Treaty. *EUCE*. Retrieved from http://www.euce.org/eusa/2011/papers/6i_nugent.pdf

Pearson, I. L. (2011). Smart grid cyber security for Europe. *Energy Policy*, 5211-5218. Retrieved from http://www.sciencedirect.com/science/article/pii/S0301421511004435

Peers, S. (2011). *EU Justice and Home Affairs Law.* Oxford: Oxford University Press. Retrieved from https://books.google.nl/books?id=X0YlF7X1mlgC&pg=PA85&lpg=PA85&hl=nl#v=onepage&q&f=false

Schjolberg, S., & Ghernaouti-Helie, S. (2009). *A Global Protocol on Cybersecurity and Cybercrime.* Oslo: E-dit. Retrieved from http://www.cybercrimelaw.net/documents/A_Global_Protocol_on_Cybersecurity_and_Cybercrime.pdf

Schwartz, F., & Talley, I. (2015, June 23). *U.S. Officials Warn Chinese Cyber Espionage Imperils Ties*. Retrieved from The Wall Street Journal: http://www.wsj.com/articles/biden-urges-honest-direct-talks-between-u-s-china-1435071461

Tikk, E. (2010). Global Cybersecurity - Thinking About the Niche for NATO. *SAIS Review of International Affairs*, 105-116. Retrieved from http://muse.jhu.edu/journals/sais_review/v030/30.2.tikk.html

Tsagourias, N. (2012). Cyber attacks, self-defence and the problem of attribution. *Journal of Conflict and Security Law*. Retrieved from http://jcsl.oxfordjournals.org/content/early/2012/07/23/jcsl.krs019.short

United Nations. (2011). *Resolution adopted by the General Assembly 66/24: Developments in the field of information and telecommunications in the context of international security.* United Nations General Assembly.

United Nations. (2013). *Comprehensive Study on Cybercrime.* United Nations Office on Drugs and Crime.

United Nations. (2013). *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.* United Nations General Assembly.

United Nations. (2014). *Resolution adopted by the General Assembly on 27 December 2013 68/243: Developments in the field of information and telecommunications in the context of international security.* United Nations General Assembly.

Wessel, R. (2015 (forthcoming)). Towards EU Cybersecurity Law: Regulating a New Policy Field. In N. Tsagourias, & R. Buchan, *Research Handbook on International Law and Cyber Space.* Cheltenham/Northhampton: Edward Elgar Publishing.

Wouters, J., Coppens, D., & Meester, B. (2008). The European Union's external relations after the Lisbon Treaty. *The Lisbon Treaty*, 143-203. Retrieved from http://www.springerlink.com/index/WM30161765862201.pdf