Universiteit Leiden

Failed to Connect

"Failed to Connect: an analysis of European decisiveness in Cybersecurity policy"

MA-Thesis International Relations - European Union Studies (IR-EUS), Universiteit Leiden

In cooperation with: TNO Strategy and Policy, subgroup Information Society

Petra Vermeulen, Student 1555391

Supervisor: Jan Oster

Table of Contents

Introduction:

Only 65 years ago, the European Integration process took off. If one would have stated then that the ECSC would result in a European Union with a single currency, European law, and free movement of capital, people, services and goods, politicians would probably say: "impossible". Yet these days the EU has all these things. However, national authorities have not given up their full sovereignty yet, making the EU a project often referred to as 'Sui Generis'.[1] With power at both supranational and intergovernmental level, the EU is unlike anything in the world: not an International Organisation, but not a true state or federation either. Instead, the EU is an increasingly complex political and social-economic landscape.

For students of International Relations, the European Union therefore forms an interesting object of study. European Union Studies aims to analyse and explore the complex EU landscape, by looking at the internal and external developments of the post-war era and examine the current state of affairs within the EU. One debate is central in this: how can European Integration best be explained, and more importantly, what does this mean for the future of the EU? In other words, where is the EU going? In this debate, two major IR-theories have emerged: Intergovernmentalism and Neo-Functionalism. Both analyse the European Integration process, but the way these theories deal with their main drivers and the future of the EU is different.

Neo-Functionalism was first set up by Ernst Haas, and considers integration to be driven by created institutions. The aim is to integrate individual sectors to achieve spill-over affects: this refers to situations where an initial decision by governments to place a certain sector under the authority of central institutions, results in pressure to extend authority of that institution to a neighbouring area of policy. Thus, Neo-Functionalism believes integration to be self-sustaining: spill-over will trigger economic and political dynamics that drive further cooperation. In other words, integration in one sector will be likely to create its own drive to spread to other sectors. Integration is therefore driven by created institutions – even if originally it was not aimed to do so.

Intergovernmentalism, on the other hand, sees states (and national governments in particular) as the main actors in the integration process. It is thus conflicting with the theory of Neo-Functionalism. Intergovernmentalism was a.o. developed by Andrew Moravcsik, who stated that any increase in power at the supranational level results from a direct decision by governments.[2] Periods of radical change in the European Union are seen to be the result of converging governmental preferences, while periods of inactivity are ascribed to diverging national interests. Intergovernmentalism further assumes that government preferences are exogenous – in other words, are not formed or changed in the course of international negotiations or by international

[1] For example: Krzysztof Feliks Sliwinski, "Moving Beyond the European Union's weakness as a Cyber-Security Agent". Contemporary Security Policy, Volume 35, Nr 3, 2014. Pages 468-486. URL: http://www.tandfonline.com/doi/abs/10.1080/13523260.2014.959261?journalCode=fcsp20#.VYqnxU3759A

[2] Andrew Moravcsik, "In Defence of the Democratic Deficit: Reassessing Legitimacy in the European Union", Center for European Studies, Working Paper No. 92, Journal of Common Market Studies, Volume 40, Issue 04, 2002, pages 603-624. URL: http://aei.pitt.edu/9136/1/Moravcsik92.pdf

institutions.[3] Summarizing, Intergovernmentalism states that the level and speed of European Integration are controlled by national governments.

This central debate is applicable at two levels. On the one hand, there is a theoretical debate about what the EU exactly entails and where it is going. On the other hand, it is also a practical debate, since Intergovernmentalism and Neo-Functionalism are existing next to each other in the EU. The question here is: should the institutions or Member States control EU integration? The outcome of this debate can be found in the different decision making procedures for different policy areas. Features of Neo-Functionalism exist in the EU's trade policy, which has been brought to the supranational level. Here, the main legislative power is the European Commission, proposals are subject to Qualified Majority Voting in the Council, and eventual decisions override national laws. However, Member States have not given up their sovereignty yet: in areas such as foreign policy and security the EU has little to no competences. In the 'special legislative procedure' applied in these policy areas, clear intergovernmentalist features exist. The most powerful body in this procedure is the European Council (heads of state or government), which votes by unanimity. At times this hybrid structure is an issue: Member States want to keep their voice in certain areas, while EU action might also be necessary to act decisive in these fields.

In this thesis, Cybersecurity will be researched as part of the central debate. In the field of Cybersecurity, the clash between decision making on the national and EU level is specifically problematic. The internet challenges the traditional Westphalia notion of sovereignty: it has created a new dimension for transnationality in which thinking in state terms will no longer suffice. To solve the problems connected to Cyberspace politicians therefore have to step away from their classical political and IR-perspectives and find solutions beyond their state. In other words, because of the transnational character of Cyberspace, the approach against Cyber related problems should also be transnational. This is especially true as the internet is ever growing, while threats are emerging more often and are getting more advanced. In dealing with them a state-by-state approach will not suffice. Although both Member States and the EU realise this, a general and overarching EU Cybersecurity policy has not yet emerged.[4] This does not mean that the EU has not done anything to address Cyberthreats: recently, a Cyber Security Strategy was launched[5], a Digital Agenda for Europe was set

[3] Jeremy Richardson and Sonia Mazey, "European Union: Power and Policy-making", Routledge, Fourth Edition, 2015, page 40. URL: https://books.google.nl/books?id=l0ihBgAAQBAJ&pg=PA39&lpg=PA39&dq=intergovernmentalism+ir&source=bl&ots=E7Zkz3oj4t&sig=hoCZAZTCoGnsO029gfx09M1gm-Q&hl=nl&sa=X&ei=X8MwVZjuBtHraq6ugMAC&ved=0CDcQ6AEwAg#v=onepage&q=intergovernmentalism%20ir&f=false

[4] European Cyber Security Protection Alliance (CYSPA), "D2.2.1 – Impact contribution and approaches – European Policies and directives", Project Number FP7-ICT-2011-8 / 318355. 31 December 2013. Page 29.

[5] European Commission (E.COM) and High Representative of the European Union for Foreign Affairs and Security Policy (HR), Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace". Brussels, 07-02-2013. JOIN (2013) 1 Final.

up[6] and a directive on Network and Information Security was issued.[7] The aim of all these policies is to ensure a high level of Network and Information Security across the EU.[8] However, the EU still receives much criticism on its policy[9], giving rise to the question whether the European strategy is in fact decisive. This thesis will look into this, by asking the research question:

"To what extent is Europe decisive in its Cybersecurity policy?"

To answer this question it is first of all crucial to define what "Cybersecurity" and "Decisiveness" exactly entails. The notion of "Cybersecurity" is not easy to define. As will be explained in Chapter two, there is no common European definition on Cybersecurity yet. The term "Cybersecurity" in this thesis should therefore be read in the broadest sense. In defining it "Cybersecurity" will be considered to be any form of protection against any sort of Cyberattack. On a scale of impact it is thus not limited to a single citizens' privacy (on the lowest level), nor to Cyberwarfare (on the highest level). Protection against Cyberbullying, Cybercrime, Cyberterrorism and Cyberwarfare therefore all fall under the umbrella of Cybersecurity.

In measuring Cybersecurity decisiveness, the definition of Cox and McCubbins will be used. Cox and McCubbins have defined "policy decisiveness" as "an ability to decide or to pursue a consistent policy", and propose several political institutional factors that determine state (in)decisiveness. First of all, they argue separation of power will lead to indecisiveness. This separation can be found between executive and legislative powers (presidentialism), within a legislative body (bicameralism) or across different levels of government (federalism). Second, independent actors in the political bargaining process make it harder to initiate and maintain collective action. Hence, so is argued, the more actors (such as parties or factions) there are in the legislature, the more indecisive the country.[10]

This definition of Cox and McCubbins is clearly set up for state decisiveness. The EU is not a state: it is, as mentioned earlier, a 'Sui Generis' institution. Nevertheless, the notion that many independent actors in the political process lead to policy indecisiveness, can also be applied in the case of the EU -

[6] The European Commission's "Digital Agenda For Europe" was launched as part of the Europe 2020 strategy. The main objective is to develop a digital single market in order to generate smart, sustainable and inclusive growth in Europe. It is made up of seven pillars. (More Info available at: http://ec.europa.eu/digital-agenda/en/digital-agenda-europe-2020-strategy)

[7] E.COM 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". Brussels, 07-02-2013. (COM)2013, 48 Final.

[8] Portal European Commission, Digital Agenda for Europe, Cybersecurity and Privacy - Cybersecurity. Available at: http://ec.europa.eu/digital-agenda/en/cybersecurity

[9] For example: Presentation by Ex-Hackers Ralf Bendrath & Florian Walther, " The EU approach to Cybersecurity and Cybercrime: From the Virtual Schengen Border to Criminalising Hacker Devices", Sigint Conference 2012 (May 2012).

[10] Definition of Cox & McCubbins as stated in Kyung Joon Han, "Policy decisiveness and responses to speculative attacks in developed countries", European Journal of Political Research, Volume 48, Number 6, 2009, pages 723-755, specifically page 730. URL: http://onlinelibrary.wiley.com.ezproxy.leidenuniv.nl:2048/doi/10.1111/j.1475-6765.2009.01835.x/epdf

and thus in this study. Just as the number of parties in the legislature affect the policy process, the number of governments and institutions in the EU structure does as well. The more parties involved in the decision making process, the more difficult it is to initiate collective action.

This thesis complements Cox and McCubbins' definition with a criterion of policy speed. As developments in the Cyberworld are rapid, acting decisive in the field of Cybersecurity means adapting quickly to these new developments. In this, an inherent supranational element can be recognized in Cybersecurity. This has implications for the policy procedure: when twenty eight states will have to reach consensus, reaching a decision will be slower than when a procedure of majority voting will be applied. Thus, speed in the decision making process is crucial for Europe's decisiveness in Cybersecurity. In answering the research question, these three criteria (separation of powers, many independent actors in the political bargaining process, and policy speed) are used extensively.

In the first chapter, the focus is on the separation of powers criterion. This chapter analyses the establishment of a common European Cybersecurity policy. To do so, a popular method among historians is used: several crucial ('watershed') moments in a relevant period of history are picked, through which the entire policy development of that period is described. In this case, four watershed moments in Cybersecurity history (1990-present) are analysed: the first EU initiative on Cybersecurity policy (1990), the first international convention on Cybersecurity (2001), the first major Cyberattack against a country (2007), and the first use of a Cyberweapon with physical damage (2010). The sub question in this part of the analysis is: "Have certain 'watershed' moments influenced Europe's Cybersecurity policy? If so, in what way?"

In the second chapter, the focus is on the amount of independent actors in the political bargaining process. In this part, the current Cybersecurity policy situation is analysed. This is done with the sub question: "What barriers exist in this current policy structure?". In doing so, the effect of bilateral agreements is also researched. In this chapter the notion that Cybersecurity in itself has a supranational element will be key.

In the third chapter, policy speed is researched. This is done by comparing the EU's policy structure in the field of Cybersecurity with that of another major Cybersecurity player: the United States. This way, a judgement about Europe's policy speed will be placed in a better context. The sub question of this chapter is: "What are the differences between the European and US Cybersecurity policy structure? Could and should the EU adopt certain parts of the US policy?"

The eventual aim of the research is to make claims about Europe's Cybersecurity policy as a whole. As a result, the scope is fairly broad. However, limitations are made in the researched region and researched policy area: the thesis only examines the European Cybersecurity policy. Thus it will not analyse global trends or developments in a single state. Naturally, an exception is made in Chapter 3, where the US Cybersecurity policy is researched – yet this is only with the aim of comparing the EU policy structure with other player. Besides limits on the geographical area, the research is Cybersecurity policy specific: it is not a general analysis of EU policy making or EU institutions.

Nonetheless, no distinction will be made within the term “Cybersecurity”, i.e. the thesis does not analyse a single aspect of Europe’s Cybersecurity policy. The reason for this is twofold:

1) As Europe has no distinction in the term “Cybersecurity”, it is extremely difficult to make such a distinction in this thesis. The domains within Cybersecurity are not strictly separated; the differences between Cybercrime, Cyberterrorism and Cyberwarfare are not always clear, nor can the measures taken against these be seen in isolation. For example: to look at Europe’s Cyberterrorism policy, one would also have to look at Europe’s Cybercrime policies and the measures taken as defence against this. Thus, only by analysing the entire Cybersecurity policy, one can draw conclusions about certain parts of this policy.

2) As Cybersecurity is relatively new, there is hardly any IR-literature available on the topic. The result is paradoxical: it is extremely difficult to study only a small portion of Europe’s Cybersecurity, as there would not be enough material available to do so. This is enhanced by the fact that most policy documents only show the outcome of discussions, rather than the actual negotiations – documents showing negotiations are still confidential and thus excluded from public use. Thus, the only option is to keep the scope broad – even if this means that the research has little limitation. However, considering the enormous literature gap in International Relations on Cybersecurity, having little limitation is not necessarily a bad thing: any conclusion contributes to a debate.

It is important to note that the lack of distinction within the term “Cybersecurity” does not mean that the research analyses everything that has even remotely to do with Cybersecurity. Several aspects are still left out of the analysis. First of all, as the research question is formulated from an IR viewpoint, the thesis merely looks at relationships among countries and the influence of sovereign states and intergovernmental organisations on a certain policy area – in this case Cybersecurity. Within the field of International Relations, the author has specialised in European Union Studies. The European Union is an increasingly complex and fascinating political and socio-economic landscape. European Union Studies aims to analyse and explore these issues, by looking at the internal and external developments of post-war Europe and examine the current state of affairs within the EU. Therefore, the thesis does not look into the business side of Cybersecurity: a Cyberattack on a certain company is only analysed if the attack resulted in a shift in state-thinking, resulting in turn in a traceable impact in EU policies (or a markedly lack thereof). Hence, the civilian side is also left out: if a single individual or a small group of individuals receives spam, this is not an issue for the EU as such. As a result, this research does not look into Data Protection, since it is highly related to civilians and the private sector. Also, much research on Data Protection and Privacy has already been conducted by practitioners of law. Data Protection thus touches upon a legal analysis, rather than an EU-wide interstate policy analysis.

Concerning methodology, this thesis provides a quantitative analysis with conclusions based on extensive research of existing literature – not just from the discipline of International Relations, but

also from the field of Law and Security Studies. Additionally, policy documents of the EU, EU Member States, and NATO will be researched. As mentioned earlier, this thesis does not take the form of a single case study, since it aims to determine the overall decisiveness of European policy on Cybersecurity, not just a response to one event. In the words of the American scientist Leroy Hood: "If you just focus on the smallest details, you never get the big picture right".[11]

[11] Leroy Hood, American Scientist, Born 10 October 1938, on Brainy Quote. URL: http://www.brainyquote.com/quotes/quotes/l/leroyhood652754.html

Chapter 1
Developing Europe's Cybersecurity policy

> **"We ignore the risks that are hardest to measure, even if they pose the greatest threat to our wellbeing." – Nate Silver, Author of 'Signal and the Noise'.**

Smartphones, e-mail, online shopping - technological developments of recent decades have affected our lives immensely. The internet has become a vital part of our society. However, online identity theft, hacking, or even Cyberwarfare, show us that the explosive growth of the internet also has a downside: it has resulted in a growing number of threats related to the digitisation of society. These threats challenge the Westphalian idea of state sovereignty, since attackers cannot easily be identified: they are no longer tied to specific states or restricted by borders. To fight these new and evolving threats, states must develop Cybersecurity strategies capable of handling challenges indicative of this new security status quo.[12] Thus, the approach against transnational cyber related problems should also be transnational. Citizens can only be protected from the dangers the internet poses, if politicians think 'beyond their state' and look for international cooperation. In this chapter, the extent of international cooperation is researched, by analysing the development of Europe's Cybersecurity policy. To do so, four watershed moments in Cybersecurity history are analysed: the first EU initiative on Cybersecurity (a Commission proposal from 1990), the first international convention on Cybersecurity (a Council of Europe Cybercrime convention in 2001), the first major Cyberattack against a country (the attacks on Estonia in 2007), and the first Cyberweapon with physical damage (the use of Stuxnet in 2010). Have any of these four moments resulted in a change of Europe's Cybersecurity policy? If so, in which way?

[12] Jared Brow, "The Need for Greater Transatlantic Cybersecurity Cooperation", Blog on Issues of International and European Security, ISIS Europe, 19 June 2014, URL: https://isiseurope.wordpress.com/2014/06/19/the-need-for-greater-transatlantic-cybersecurity-cooperation/

1990: the first initiative

When Cyberspace was still in its infancy, the EU's Cybersecurity policy was subject to the control of national governments. This is first of all visible in the early suggestions for an EU Cybersecurity policy. In 1990, the European Commission issued a first proposal to treat Cybersecurity as a separate policy area. In this, the Commission expressed far-reaching ambitions to get 'Information Security' to the EU level.[13] According to the document, the security of Information Systems was essential for the functioning of the Internal Market – thus the Commission should be the main decision maker in this area and receive the competence for decision making. As the 1990 text states:

> "The diversity of national approaches and the lack of a system of protection at Community level are an obstacle to completion of the Internal market. (…) A Community approach towards the protection of individuals in relation to the processing of personal data is (…) essential to the development of the data processing Industry and of value-added data communication services."[14]

The document includes a long list of underlying values to legitimize EU policymaking, such as the protection of privacy, intellectual property, commercial confidentiality, and national security. Based on this list, the Commission argues that the ordinary legislative procedure should be used as the main decision making process. In this so-called 'Community method' the Commission is the main legislator, the European Parliament has amendatory powers, and the Council votes by Qualified Majority Voting (QMV). The wish for such a supranational decision-making procedure is explicitly stated in the plan:

> "The proposed approach is designed to ensure a high level of protection via a **Community system** of protection, based on a set of complementary measures." [15]

However, this supranational Community Method would not be achieved, as the Council of Ministers (representing the national governments) considerably tempered the Commission's plans in 1992. Member States were not convinced that giving up sovereignty in the field of Cybersecurity would be

[13] COM(90) 314 final, OJ C 277/18, 5 November 1990, page 18 - in Axel Arnbak, "Any Colour You Like: the History (and Future?) of E.U. Communications Security Policy", IViR/Berkman Roundtable, 18 April 2014, page 4

[14] Commission of the European Communities, "Commission Communication on the Protection of Individuals in relation to the processing of personal data in the Community and Information Security", COM(90) 314 final – SYN 287 and 288, Brussels, 13 September 1990, URL: http://aei.pitt.edu/3768/1/3768.pdf

[15] Commission of the European Communities, "Commission Communication on the Protection of Individuals in relation to the processing of personal data in the Community and Information Security", COM(90) 314 final – SYN 287 and 288, Brussels, 13 September 1990, URL: http://aei.pitt.edu/3768/1/3768.pdf

in their best interest. The Council stated that the proposal evoked the subsidiarity principle* in the preambles, and should be removed. This supports the Intergovernmentalism notion that the level and speed of European Integration in the field of Cybersecurity is determined by National Governments. Several of the other changes made to the Commission Document also back this theory. For example, the argument that Information Security was part of the Internal Market was found invalid. Another alteration included more representation of Member States in the Expert Group and the final say of the Council in cases of conflict. More importantly, the Council's changes included a right to postpone actions suggested by the Commission.[16] With this, the Commission effectively lost all executive power. The result was a clear setback of Cybersecurity to the Intergovernmental level. As Axel Arnbak has stated: "With the 1992 Council Decision, Member states claimed control of network and information security policy making".[17]

At the time, however, keeping Cybersecurity at the national level was not yet problematic. In 1992, the World Wide Web was only three years old - commercial use of the internet would not be introduced until 1995.[18] Internet was still in its infancy – although threats occurred, the impact was limited, as only a limited number of people were connected to the internet. Thus, for the time being, national control sufficed.

* The subsidiarity principle ensures that decisions are taken as closely as possible to the citizen and that constant checks are made to verify that action at Union level is justified in light of the possibilities available at national, regional or local level. Specifically, it is the principle whereby the Union does not take action (except in the areas that fall within its exclusive competence), unless it is more effective than action taken at national, regional or local level. It is closely bound up with the principle of proportionality, which requires that any action by the Union should not go beyond what is necessary to achieve the objectives of the Treaties.

[16] Council Decision 92/242/EEC, In the Field of Security of Information Systems, Annex - Summary of action lines, Official Journal of the European Communities, 31 March 1992. URL: http://policy.mofcom.gov.cn/english/flaw!fetch.action?id=056235c9-75d6-4070-9a78-ab605e3ae84c

[17] Axel Arnbak, "Any Colour You Like: the History (and Future?) of E.U. Communications Security Policy", IViR/Berkman Roundtable, 18 April 2014, page 4.

[18] YanTian and Concetta Stewart, "History of E-Commerce", in: Mehdi Khosrow-Pour, "Encyclopedia of E-Commerce, E-Government and Mobile Commerce", IGI Global, 2006, page 560.

2001: CoE Convention – Progress… Yet Not.

In the 2000's the situation had changed to some extent. In ten years' time, the number of West-European internet users had grown to 20,4%.[19] With the growing interconnectivity, the plea for international cooperation grew as well. To this end, a Cybercrime convention was organised in the Council of Europe in 2001 (note: the European Council and Council of Europe are two different institutions[*]). The convention would give Europe's Cybersecurity legislation a huge boost: much of today's EU Cybercrime legislation still finds its origins in this convention. Some progress thus seemed to be made. However, it is wrong to consider this the end of Member State control. To clarify this: in 2002, the Commission issued a proposal implementing some of the major idea's from the convention. In this, the Commission copied much of the wording of the 'Threats to Information Systems' proposal from 1990.[20] However, the Member States once again discouraged this wording: although the Council Decision confirmed the idea of Cybercrime legislation at the EU level, some major points were excluded. For instance, a terrorist attack on information systems was excluded from "Cybercrime", as this touched too closely upon the notion of national safety.[21] Terrorism was considered to be part of the exclusive area of national security – and thus its digital counterpart was also exempted from EU competence.[22] Hence, Intergovernmentalism theory can again be confirmed here - governments remained the main drivers in the (Cybersecurity) integration seat: despite new legislation, power remained at the national level, continuing the line of government control.

[19] Pippa Norris, "Digital Divide: Civic Engagement, Information Poverty, and the Internet Worldwide", Cambridge University Press, 24 September 2001, page 47, figure 3.1: The Percentage of the Population Online by Major Region in 2000.

[*] The Council of Europe (CoE) is an international organisation of which 47 European countries are members. In addition, six non-European countries (as well as the Vatican) observe in the CoE. The European Council, on the other hand, is the institution mentioned before, in which the 28 Heads of State or Government of EU Member States are represented.

[20] Commission of the European Communities, 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", Brussels, 06 June 2001, COM(2001) 298 final, page 9

[21] Axel Arnbak, "Any Colour You Like: the History (and Future?) of E.U. Communications Security Policy", IViR/Berkman Roundtable, 18 April 2014, page 18.

[22] Axel Arnbak, "Any Colour You Like: the History (and Future?) of E.U. Communications Security Policy", IViR/Berkman Roundtable, 18 April 2014, page 18.

2007: Estonia

In the spring of 2007, the notion of arranging Cybersecurity on the national level was severely challenged for the first time, when Estonia became the target of a major Cyberattack. The events in Estonia shocked the world: websites of Estonian organizations, banks, parliament, ministries, newspapers and broadcasters were flooded with data (some sort of "Data Tsunami"), leaving them inaccessible for nearly three weeks. Not only was this the first Cyberattack on such a major scale and continuing for such a long time, it was also the first time that a Cyberassault occurred against a state. Many suspected Russia to be behind the attacks, since they had started after commotion about Estonian removal of a Bronze Soviet war memorial in Tallinn. Also, the attacks gradually intensified, with the number of attacks being the biggest on the 9th of May – the day that Russians commemorate Hitler's defeat in Europe. Soon, therefore, media started to label the attacks as "the first case of Cyberwarfare".[23]

As Estonia was both a member of the EU and NATO, both of these parties were obliged to respond quickly. However, neither had protocols for such a situation. After all, up to the 2007 attacks, national control (Intergovernmentalism) had proved to be sufficient to deal with Cyberthreats. However, from 2007 onwards, this was no longer the case – Cybersecurity could clearly only be dealt with by international cooperation. For NATO, especially, Estonia proved to be a wake-up call.[24] With the alleged Russian involvement, Cyberwarfare was no longer just a future scenario – NATO had to decide whether or not they would frame Cyberattacks under Article V, which provides a collective self-defence system as soon as a NATO member state is attacked.[25] However, some NATO members remained cautious, stressing the importance of national sovereignty. NATO was able to solve the framing-problem in a relatively short period of time (first framework set up in June 2007, actual implementation of the strategy in 2008).[26] The solution to the Article V problem was to frame Cyberattacks under Article IV, which states that: "…parties will consult together whenever, in the opinion of any of them, the territorial integrity, political independence or security of any of the Parties is threatened".[27] With this solution, NATO elevated Cyberattacks to warfare status, but it did so under a framework of collaboration and consulting, rather than an automatic collective response to an attack against a NATO member.[28]

---

[23] Ian Traynor, "Russia accused of unleashing cyberwar to disable Estonia", the Guardian, World News, Brussels, 17 May 2007, URL: http://www.theguardian.com/world/2007/may/17/topstories3.russia

[24] Kertu Ruus, "Cyber War I, Estonia Attacked from Russia", The European Institute, published in: European Affairs, Volume 9, Issue 1-2, Winter/Spring 2008. URL: http://www.europeaninstitute.org/index.php/component/content/article?id=67:cyber-war-i-estonia-attacked-from-russia

[25] North Atlantic Treaty Organization (NATO), "The North Atlantic Treaty", Official Text, Article 5, Washington D.C., 4 April 1949, URL: http://www.nato.int/cps/en/natolive/official_texts_17120.htm

[26] Joshua McGee, "NATO and Cyber Defense: A Brief Overview and Recent Events", Center for Strategic and International Studies (CSIS), 8 July 2011, URL: http://csis.org/blog/nato-and-cyber-defense-brief-overview-and-recent-events

[27] North Atlantic Treaty Organization (NATO), "The North Atlantic Treaty", Official Text, Article 4, Washington D.C., 4 April 1949, URL: http://www.nato.int/cps/en/natolive/official_texts_17120.htm

[28] Scheherazade S. Rehman, "Estonia's Lessons in Cyberwarfare", USNews.com, 14 January 2013, URL: http://www.usnews.com/opinion/blogs/world-report/2013/01/14/estonia-shows-how-to-build-a-defense-against-cyberwarfare

In the EU however, though Estonia proved to be a wake-up call regarding the severity of threats, the long term policy implications were slow and limited. Where NATO had a solution to the Article V problem in two months, the EU did not present new solutions to Cyberthreats up to 2010.[29] Also, the EU's answers came mainly in the form of new laws, rather than an actual switch in policy making. For example, in November 2010, the EU released its Internal Security Strategy, calling for an integrated responses to Cybersecurity threats and significantly expanding the European Network and Information Security Agency's responsibilities (beyond its previously limited analytical role). The EU also launched a new Digital Agenda for Europe, which included plans to establish CERTs* for EU institutions, hold multinational Cyberdefence simulations, and create a joint European Cybercrime platform.[30] It thus might seem as if the EU released its Intergovernmental character of Cybersecurity policy. On closer inspection, however, both initiatives clearly show a national grip on Cybersecurity.

The first initiative, the Internal Security Strategy, was launched in the AFSJ* framework. This suggests that the Commission was the main actor in the legislation process. However, the strategy was adopted under Article 68 TFEU, which states that: "The European Council shall define the strategic guidelines for legislative and operational planning within the Area of Freedom, Security and Justice".[31] Although the Internal Security Strategy was adopted under the AFSJ, the main actor in power was thus the European Council. As the European Council decides by consensus rather than by Qualified Majority Voting, each Member State (in line with Intergovernmentalism theory) kept their voice in Cybersecurity matters. I.e., power remained with the Member States.

The second initiative, the Digital Agenda for Europe (including the CERTs proposal) was adopted as part of the Europe2020 strategy. This strategy is rooted in a policy and legislation procedure known as the Open Method of Coordination (OMC).[32] The OMC was set up in 2009 as a new framework for cooperation between the Member States to direct national policies towards certain common objectives. Under this intergovernmental method, Member States are evaluated by each another (peer pressure), and the Commission's role is limited to surveillance.[33] This once again shows the power of the Member States in the area of Cybersecurity – if Member States don't achieve the goals they agreed upon, no harsh sanctions will follow. The conclusion can thus be clear: Estonia provided a wake-up call, but no real policy shift took place - new legislation was issued, but decision making was kept on the intergovernmental level.

---

[29] Stephen Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses", Journal of Strategic Security, Volume 4, Number 2: Strategic Security in the Cyber Age, Summer 2011, page 55. URL: http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1105&context=jss

* CERTs, Computer Emergency Readiness Teams, acts as a primary Security Service Provider for both Governments and Citizens. As ENISA states, they work like a fire brigade: they are the only ones which can react when a security incident occurs. It thus mostly acts as a reactive service: incident response.

[30] Stephen Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses", Journal of Strategic Security, Volume 4, Number 2: Strategic Security in the Cyber Age, Summer 2011, page 55. URL: http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1105&context=jss

* AFSJ is short for Area of Freedom Security and Justice

[31] Consolidated Version of the Treaty on the Functioning of the European Union (TFEU) Article 68, in: Nigel Foster, "Blackstone's EU Treaties & Legislation 2014-2015", Oxford University Press, 25th Revised edition, August 2014.

[32] European Union Committee of the Regions, "Digital Agenda For Europe, the role of regions and cities", Background note Conference of the Committee of the Regions, Brussels, 2 July 2013, page 5. URL: http://cor.europa.eu/en/news/events/Documents/digital_agenda_background.pdf

[33] Europa, Synthèses de la législation, Glossary, "Open Method of Coordination", URL: http://europa.eu/legislation_summaries/glossary/open_method_coordination_en.htm

2010: Stuxnet

In Estonia, servers of websites were flooded with data, causing serious inconvenience, yet no physical damage was done. This changed in 2010 when a computer worm known as Stuxnet targeted Industrial and Factory control systems for the first time. Stuxnet was significant – not only because it was (as Alan Bentley, senior international vice president at security firm Lumension has stated) "the most refined piece of malware ever discovered", but also because "mischief or financial reward wasn't its purpose – it was aimed right at the heart of Critical Infrastructure*".[34]

In January 2010, inspectors of Iran's Natanz uranium enrichment plant noticed that centrifuges used to enrich uranium gas were spinning out of control. The cause was a mystery – Iranian technicians replaced the centrifuges but neither them, nor the inspectors observing the centrifuges understood where the problem was coming from. Circa five months later a similar event took place. A computer security firm from Belarus was called in when a series of computers was repeatedly crashing and rebooting. After an extensive search, the researchers found a few malicious files on one of the systems. Stuxnet, as the malware became known, was unlike any other virus or worm ever seen before. Technically, the malware was extremely advanced. To explain this more technical story: the worm only looked for a specific piece of hardware in industrial systems – only if a certain chip would be found in a system, the worm would be triggered. Typically, the chip the worm was looking for was made by Siemens and used in factory floors, chemical plants and nuclear power plants.[35] As this specific Siemens-chip was assumed to be used in Iran's Nuclear enrichment facilities, suspicions were made soon after the attack that Stuxnet was aimed specifically at Iran's Nuclear programme. Another Stuxnet characteristic was that it did not threaten with sabotage, like a criminal organization would do, but instead performed sabotage itself - rather than simply hijacking targeted computers or stealing information from them, Stuxnet escaped Cyberspace to wreak physical destruction on equipment the computers controlled.[36] In the end, Stuxnet eliminated approximately one fifth of Iran's nuclear centrifuges and significantly hampered Iran's ability to make its first nuclear arms.[37] With this, Stuxnet became the first Cyber weapon in history to cause physical damage.

For Europe, Stuxnet resulted in the classic paradox that we have seen before: more awareness, yet holding on to national control. Initially, Europe was shocked by Stuxnet. The European Network and Information Security Agency (ENISA) stated in its initial comment that Stuxnet was "really a

---

* Critical Infrastructure is a term used by governments to describe assets that are essential for the functioning of a society and economy. Most commonly associated with the term are facilities for electricity generation, water supply, telecommunication, transportation systems, financial services, etc.

[34] Josh Halliday, "Stuxnet worm is the 'work of a national government agency'", The Guardian, 24 September 2010, URL: http://www.theguardian.com/technology/2010/sep/24/stuxnet-worm-national-agency

[35] Bruce Schneier, "The Story Behind The Stuxnet Virus", Forbes, 07 October 2010, URL: http://www.forbes.com/2010/10/06/iran-nuclear-computer-technology-security-stuxnet-worm.html

[36] Kim Zetter, "An Unprecedented Look At Stuxnet, The World's First Digital Weapon", Wired, 11 March 2014, URL: http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

[37] William J. Broad, John Markoff and David E. Sangerjan, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay", New York Times, 15 January 2011, URL: http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=0

paradigm shift, as it is a new class and dimension of malware." [38] The executive director of ENISA, Dr. Helmbrecht, even said:

> "After Stuxnet, the currently prevailing philosophies on Critical Information Infrastructure Protection (CIIP) will have to be reconsidered. They should be developed to withstand these new types of sophisticated attack methods. Now that Stuxnet and its implemented principles have become public, we may see more of these kinds of attacks. All security actors will thus have to be working more closely together and develop better and more coordinated strategies."[39]

It thus might seem as if Stuxnet resulted in more coordination at last. To some extent Stuxnet was indeed a paradigm shift for the EU– as Stuxnet had targeted so called "Critical Infrastructure", Europe feared a similar attack. After Stuxnet, many EU Member States classified Cyber as the 5th domain of Warfare, established dedicated Cyber Commands, and/or set up National Cyber Strategies. This can be made apparent from the fact that most Cybersecurity strategies date back to 2011 – with exception of Estonia, which set up a strategy in 2008, which is notably one year after the DDOS-attacks.[40] On the EU level, however, not much changed. One explanation for the little impact of Stuxnet on the EU level, could be that Stuxnet was a Cyberweapon with a physical target, aimed to destruct Critical Infrastructure. As will be argued further in chapter two, this makes it more NATO's discipline than that of the EU. Where the Estonia attack mostly had a civilian target (banks, ministries, accessibility to the internet for the general public), the Stuxnet attack had much more of a military target: it was a specific attack against a facility with great strategic value – proven by the fact that it helped delay Iran's ability to make nuclear arms.[41]

In explaining the lack of tangible EU response to the Stuxnet attacks, it is also important to note that Europe had already made plans for Critical Infrastructure Protection before the 2010 Stuxnet attacks. For example, in 2009, the Commission issued the Communication "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security, and resilience". In this proposal, the Commission defined a plan for immediate action to strengthen the resilience of Critical

---

[38] ENISA, "EU Agency analysis of 'Stuxnet' malware: a paradigm shift in threats and Critical Information Infrastructure Protection" Press Release ENISA, 7 Oct 2010. URL: https://www.enisa.europa.eu/media/press-releases/eu-agency-analysis-of-2018stuxnet2019-malware-a-paradigm-shift-in-threats-and-critical-information-infrastructure-protection-1

[39] ENISA, "EU Agency analysis of 'Stuxnet' malware: a paradigm shift in threats and Critical Information Infrastructure Protection" Press Release ENISA, 7 Oct 2010. URL: https://www.enisa.europa.eu/media/press-releases/eu-agency-analysis-of-2018stuxnet2019-malware-a-paradigm-shift-in-threats-and-critical-information-infrastructure-protection-1

[40] The European Parliament Briefing "Cyber Defence in the EU: Preparing for Cyber Warfare?", European Parliamentary Research Service (EPRS), October 2014. URL: http://epthinktank.eu/2014/10/31/cyber-defence-in-the-eu-preparing-for-cyber-warfare/. Document states that Finland, France, Germany, Lithuania and the UK all set up National Cyber Policies in 2011. Additionally, the Netherlands, Denmark and Italy set up strategies in 2012 and 2013.

[41] William J. Broad, John Markoff and David E. Sangerjan, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay", New York Times, 15 January 2011, URL: http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=0

Infrastructures.[42] In this sense, we can see a similar trend as with Estonia: the event might have speeded up parts of pending legislation, but an actual policy shift stayed out. The overall decision making in the field of Cybersecurity was kept at the intergovernmental level. Even ENISA recognized this: spokesman Ulf Bergstrom stated that it is fundamentally up to each Member State to decide upon the implementation of a security policy. In explaining this, Bergstrom says "ENISA sees itself as a Matchmaker or Switchboard of best (security) practices, and what practices could work better in which Member State." [43]

[42] European Commission Communication to the European Parliament, Council, European Economic and Social Committee and the Committee of the Regions, "Protection Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience", Brussels, 30 March 2009, COM(2009) 149 final. URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF

[43] Jack Clark, "Stuxnet threat rings EU alarm bells", ZDNet, October 2010, URL: http://www.zdnet.com/article/stuxnet-threat-rings-eu-alarm-bells/

Chapter Summary

To conclude, the theory of Intergovernmentalism explains best why Cybersecurity is dealt with the way that it is: Member States view Cybersecurity as part of their national security strategies, rather than something that should be dealt with at the EU level. In the 1990s and early 2000s, Commission proposals to get Cybersecurity to the EU level were therefore rejected. At the time, a national approach might have been sufficient to deal with threats. However, the 2007 Cyberattacks on Estonia and the 2010 Stuxnet disruption have made the EU and its Member States realise that more coordination and cooperation is necessary. Strangely, however, this realisation has not resulted in a transfer of competences to the EU level. The amount of (pending) legislation in the field has increased – but no actual policy shift can be found. In this, we can clearly recognize the Intergovernmentalism notion that Member States are the main actors in the integration process: national leaders continue to view Cybersecurity as part of their national security strategies - and thus something they want to keep their grip on. Although international cooperation was sought more often after the 2007 and 2010 attacks, the national character of Cybersecurity was sustained. After 2007, governmental preferences converged to some extent, but not enough to get Cybersecurity to a supranational decision making procedure. Power remained separated over the 28 Member States. Perhaps, as Nate Silver has stated, the EU Member States choose to “ignore the risks that are hardest to measure, even if they pose the greatest threat to their wellbeing”. However, the implications of keeping Cybersecurity on the intergovernmental level would be huge – why and how this is the case, will be explained in chapter two.

Chapter 2
Chaos without Coordination

> **"In any moment of decision, the best thing you can do is the right thing, the next best thing is the wrong thing, and the worst thing you can do is nothing." – Theodore Roosevelt, 26th US President.**

Although Roosevelt's statement was made more than a century ago, it is still relevant for policy making today. The interconnected world we live in, is bursting with opportunities– but it also threatens our security in an unprecedented way. This borderless security challenge deems an active international approach. Estonia and Stuxnet have made Europe realise this. Thus, a number of initiatives have been launched by various EU institutions as well as by Member States. For example, The Netherlands launched a Defence Cyber Strategy, Germany has a National Cyber Security Council and Response Centre, and France has an Information System Defence and Security Strategy. From the EU level a Cyber Security Strategy has also been launched. Nevertheless, this might not be enough. In this chapter, the current Cybersecurity policy situation is therefore researched. The sub question in this chapter is "What barriers exist in this current policy structure?". In researching this, the second criterion for decisiveness (amount of independent actors) of Cox and McCubbins is central.

Barrier 1: Willingness to share information

A first barrier in Cybersecurity policy is that Member States have little willingness to share information on Cyberthreats. The willingness to share information between Member States is key: a single EU Cybersecurity policy can only be set up when parties actively share information on threats. Currently, sharing information is often a matter of "quid pro quo". Only if party X shares something with party Y, Y will also share something with X.[44] This passive form of cooperation is in sharp contrast with the active cooperative attitude that Cybersecurity (due to its transnational character) demands. Pro-active information sharing is essential for a decisive EU strategy – keeping Cybersecurity on national level will result in all Member States being vulnerable.[45] This is especially true since (unlike classic attacks) Cyberattacks can be difficult to trace.[46] The attackers nationality can differ from the place where he or she carries out the attack. The computer the attacker operates from could have a server in another country. The country the attacker attacks, could differ from all of these countries. To complicate things further attackers usually use IP spoofing[*] or a hidden IP address. As a result of all these factors tracing the attacker might be extremely difficult. Only by sharing information multi-nationally these issues can be tackled. This way tracing and prosecution can be made feasible.

An example of this the Cyberattack "Operation Payback", carried out in 2013. Under this operation, the websites of MasterCard and PayPal, the Swedish Public Prosecutor and Swiss Postbank were targeted by WikiLeaks sympathizers. After a few days, a Dutch teenager was arrested in the Netherlands – but the possibility of more hackers being involved outside the Netherlands was not ruled out.[47] The example shows both the perks and need for international cooperation: in this case, the situation turned out satisfactory - due to international cooperation and information sharing, the Dutch authorities were quick to arrest the teenager and bring him to (Dutch) court. However, what would happen if this was not a Dutch teenager? What if an Hungarian teenager would hack the Swiss bank from a computer in Paris, while using the IP of a Dutch computer and a server in Italy? This would complicate the tracing process - if countries do not share information, the hacker could easily remain hidden or flee the state they performed the attack from. This is made worse by the fact that there is no obligation for Member States to share information on a European level.[48]

---

[44] H.A.M. Luijf et al., "Cross-Sector Information Sharing", TNO 2014 R10945, TNO Rapport for the Dutch Ministry of Security and Justice, Project Number 032 32715, June 2014, Page 25.
[45] H.A.M. Luijf et al., "Cross-Sector Information Sharing", TNO 2014 R10945, June 2014, Page 25.
[46] Kenneth Geers, Darien Kindlund, Ned Moran, Rob Rachwald, "World War C :Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks", FireEye, September 2013, URL: http://www.fireeye.com/resources/pdfs/fireeye-wwc-report.pdf
[*] The basic protocol for sending data over the Internet network and many other computer networks is the Internet Protocol (IP). When IP spoofing is used, an attacker makes the victim believe that he sends data from another (trusted) computer than actually is the case. The technique is thus based on the falsification of the identity of a different computer, and is particularly effective when the fictitious identity is that of an entity trusted by the attacked computer.
[47] Wilbert de Vries, "Aanval op Mastercard.com werd vanuit Nederland opgezet", Tweakers, 8 december 2010, URL: http://tweakers.net/nieuws/71230/ddos-aanval-op-mastercard-punt-com-werd-vanuit-nederland-opgezet.html
[48] Europol, "The Internet Organised Crime Threat Assessment (iOCTA) 2014", European Cybercrime Center EC3 Europol, European Police Office, 2014. Page 14. URL: https://www.europol.europa.eu/ec3

Barrier 2: No Common Definition

A second barrier is that there is no common definition on what "Cybersecurity" or "Cyberattack" exactly entails. Currently, the terms are being used for (defence against) all sorts of attacks. There is no clear distinction between Cyberwarfare, Cyberterrorism, Cyberespionage, Cyberintrusion or Cybercrime. Furthermore, there is no distinction between attacks from private individuals (in the legal sense of the word) against other private individuals, attacks from states against other states, private individuals against the state, and states against private individuals.[49] Here, a major problem comes up: as the EU has no distinction between these forms of Cyberattacks, deciding who should act on which sort of attack is made difficult. The result is a blurry picture of who should act in which case. For example, attacks from private individuals against other private individuals should be dealt with by national courts, while attacks from states against other states should be dealt with at the international level. In the same way, Cybercrime would be a matter for Europol, while Cyberwarfare would be more of NATO's domain. Currently, however, each party takes up topics they feel are 'in their area'. As a result, various divisions between the EU Member States,[50] EU Institutions,[51] and EU - NATO have come up. Although the need for a single definition has been addressed by ENISA[52], the 2013 EU Cyber Security Strategy has failed to provide one. [53] In the coming section, an analysis of the resulting divisions will be made, by looking at the EU policy from three levels: EU-NATO, EU-MS, and within the EU.

[49] Erki Kodar, "Applying the Law of Armed Conflict to Cyber Attacks: From the Martens Clause to Additional Protocol", ENDC Proceedings, Volume 15, 2012, pages 107–132. URL: http://www.ksk.edu.ee/wp-content/uploads/2012/12/KVUOA_Toimetised_15_5_Kodar.pdf

[50] Bouwman and Marácz "Nederland moet inzetten op international cybersamenwerking", Atlantisch Perspectief, Number 6, 2012, pages 22-27. URL: http://www.atlcom.nl/ap_archive/pdf/AP%202012%20nr.%206/Bouwman%20en%20Maracz.pdf

[51] European Cyber Security Protection Alliance (CYSPA), "D2.2.1 – Impact contribution and approaches – European Policies and directives", Project Number FP7-ICT-2011-8 / 318355. 31 December 2013.

[52] Nicole Falessi et al., "National Cyber Security Strategies: An Implementation Guide", European Union Agency for Network and Information Security (ENISA), December 2012, URL: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-an-implementation-guide

[53] E.COM, "Cybersecurity Strategy of the European Union: An Open, Safe, and Secure Cyberspace", Joint Communication to the European Parliament, the Council, The European Economic and Social Committee and The Committee of the Regions, JOIN(2013) 1 Final., Brussels, 8 February 2013, URL: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

Barrier 3: Three levelled division

1) Division between EU and NATO

The division of policies between EU and NATO is not problematic, but even necessary to prevent the EU from getting into NATO's domain. The EU has no military division - not in the conventional sense, nor for Cyberspace. NATO, on the other hand, is exclusively set up as a military alliance, in which members are committed to collective security and common defence.[54] This distinction should be continued in Cyberspace. It makes sense for NATO to take up Europe's Cybersecurity and Cyberdefence in the case of Cyberwarfare and state-sponsored attacks. NATO has already defined Cybersecurity in a narrow way, relating to the basic functions of the alliance: the protection of NATO-networks, setting Cyberdefence requirements, and ensure collective defence and crisis management.[55] However, due to this narrow interpretation, EU action will also be necessary. Civilian aspects such as privacy, hacking and DDOS-attacks still have to be coped with, but are not in line with the military objective of NATO. The EU should therefore take up these civilian aspects. Naturally, some Cyberattacks will be hard to classify. Thus, coordination between EU and NATO is necessary to prevent policies from not being executed at all. In general, a prudent approach would be if each of the two would take up the topics deemed relevant, and seek coordination from there. It would be better for topics to be initially handled by both parties than not at all.

2) Division between EU and Member States

The case of division between EU and Member States is different from the EU-NATO division. In this case, division is difficult: the fact that policies are issued from both the EU and MS level, undermines a general EU policy. As stated by Cox and McCubbins, "many independent actors" will decrease policy decisiveness. [56] In this case, both the EU and Member States are managing Cybersecurity policy, which causes confusion about who should act in which case. This is especially true as Cybersecurity policies from Member States are not uniform. Practically all Member States have adopted a national Cybersecurity strategy[57], but the content of these strategies varies from Member State to Member State.[58] For example: around 15 Member States have introduced military Cybersecurity strategies. The other 12 Member States have addressed Cybersecurity through the

---

[54] North Atlantic Treaty Organization (NATO), "The North Atlantic Treaty", Washington D.C., 4 April 1949, URL http://www.nato.int/cps/en/natolive/official_texts_17120.htm

[55] Krzysztof F. Sliwinski, "Moving Beyond the European Union's Weakness as a Cyber-Security Agent - The EU as a Cyber Security Agent", Contemporary Security Policy, Volume 35, Issue 3, 2014. Pages 468-486. URL: http://www.tandfonline.com/doi/abs/10.1080/13523260.2014.959261#.VSOLCvmsVqU

[56] Definition of Cox & McCubbins as stated in Kyung Joon Han, "Policy decisiveness and responses to speculative attacks in developed countries", European Journal of Political Research, Volume 48, Number 6, 2009, pages 723-755, page 730. URL: http://onlinelibrary.wiley.com.ezproxy.leidenuniv.nl:2048/doi/10.1111/j.1475-6765.2009.01835.x/epdf

[57] European Union Agency for Network and Information Society (ENISA), "National Cyber Security Strategies in the World", ENISA National Cyber Security Strategies, URL: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world

[58] Wolfgang Röhrig, "Viewpoints: Cyber Security and Cyber Defence in the European Union", European Defence Agency (EDA), EDA Info Hub, Opinion. Brussels, 11 June 2014, URL: https://www.eda.europa.eu/info-hub/opinion/2014/06/11/viewpoints-cyber-security-and-cyber-defence-in-the-european-union

national security strategies already in place, if addressed at all.[59] The national descriptions differ from case to case – again partly due to the absence of a common definition over what Cybersecurity or Cyberattack entails.

These differences are problematic as they hinder the establishment of an EU-wide Cybersecurity approach. Member State X might prefer policy A, while Member State Y favours policy B. The situation thus seems to turn in circles: as there is no common EU definition and strategy, Member States have set up their own - however, this in turn hampers the establishment of a European policy. Also, the fact that national strategies received more attention than a common EU approach again underlines Intergovernmentalism theory.

3) Fragmentation between EU institutions

A third form of division exists between EU institutions.[60] This is a crucial problem for the EU's Cybersecurity policy, for internal fragmentation ("many independent actors") will result in a decrease in decisiveness according to Cox and McCubbins.[61] Currently, actions appear to be carried out by whoever finds a gap in their specific field (telecom, transport, crime, etc.). Here, the effect of the lack of a single definition is clearly visible: it is unclear who should act in which case of Cybersecurity, and thus, each party takes up topics they deem relevant. In itself, this random take up of action is not a bad thing – similar to the coordination between EU and NATO, it is better to take up topics deemed relevant and seek coordination from there, than not to take up topics at all. However, while the number of EU institutions involved in Cybersecurity is extensive, there is no single point of policy coordination from which action takes place. A Cybersecurity Coordination Group (CSCG) was set up in 2011, but this group only translates Cybersecurity policy into standards that contain technical details. It thus only functions as a technical point of coordination, not a point of coordination for policy.[62] Consequently, a patchwork of EU institutions seem to work in policy chaos, without coordination. To illustrate this, the following section will provide a short summary of the current institutional landscape.

The first institution bearing relations with the EU Cybersecurity strategy is the Directorate-General Communications, Networks, Content and Technology (DG CONNECT). DG CONNECT issued a Digital Agenda For Europe in 2010, which included CERTs for EU institutions and the creating of a joint

---

[59] Krzysztof F. Sliwinski, "Moving Beyond the European Union's Weakness as a Cyber-Security Agent - The EU as a Cyber Security Agent", Contemporary Security Policy, Volume 35, Issue 3, 2014. Pages 468-486. URL: http://www.tandfonline.com/doi/abs/10.1080/13523260.2014.959261#.VSOLCvmsVqU

[60] European Cyber Security Protection Alliance (CYSPA), "Deliverable 2.2.1 – Impact contribution and approaches – European Policies and Directives". FP7-ICT-2011-8 / 318355, 01-10-2012, page 5.

[61] Definition of Cox & McCubbins as stated in Kyung Joon Han, "Policy decisiveness and responses to speculative attacks in developed countries", European Journal of Political Research, Volume 48, Number 6, 2009, pages 723-755, page 730. URL: http://onlinelibrary.wiley.com.ezproxy.leidenuniv.nl:2048/doi/10.1111/j.1475-6765.2009.01835.x/epdf

[62] CEN / CENELEC, "European Standardization: Cybersecurity" , CEN-CENELEC Sectors: Defence, Security and Privacy – Security. URL: http://www.cencenelec.eu/standards/Sectors/DefenceSecurityPrivacy/Security/Pages/Cybersecurity.aspx

European Cybercrime platform (launched from the European Council level, see chapter 1).[63] A second institution dealing with Cybersecurity is ENISA, which enhances the capability of the EU, Member States and business community to prevent, address and respond to network and information security problems.[64] The main goal of ENISA is to "Achieve global Cybersecurity through collaboration by acting as a body of expertise to execute technical and scientific tasks in the area of information security, and helping the European Commission in the technical preparatory work for updating and establishing EU legislation".[65] It thus assists Member States in developing national Cyberresilience capabilities. A third institution is Europol's Cyber Crime Centre (EC3). Its objective is to broaden and incorporate further expertise in specialised areas. Then there is DG MOVE, the EU's institution dealing with transport and mobility issues, which in 2013 launched a call for a study on Cybersecurity in land transport. DG HOME in turn deals with various policy issues regarding European Cybercrime policy, working with Europol, ENISA and the European Cyber Crime Centre. DG Enterprise and Industry aims to protect citizens in Europe and society from harm, through research and Development. Finally, the European External Action Service (EEAS) acts as the EU's diplomatic service and can thus act as an interface between the EU Cyber strategy and Non-EU Strategies.[66]

Clearly, this division in Cybersecurity policy executers results in an opaque and complicated landscape, in which it is hard to grasp who is responsible for which policy. A policy study commissioned by the European Parliament stated that the exercise was "undoubtedly highly complex", and in the end dodged the question of a regulatory framework at hand.[67] To address the problem, the EU in 2013 launched its "European Cyber Security Strategy of the European Union: An Open, Safe and Secure Cyberspace" (EU CSS).[68] This strategy was supposed to outline the EU's vision on Cybersecurity by clarifying roles and responsibilities, and propose specific activities at the EU level. The goal was to ensure strong and effective protection and promotion of citizens' rights so as to make the EU's online environment "the safest in the world".[69] However, as the (commercial) European Cyber Security Protection Alliance (CYPSA) report states, the strategy failed to address the problem of fragmentation in the EU:

---

[63] European Commission, "Digital Agenda for Europe", Digital Agenda for Europe - A Europe 2020 Initiative, URL: http://ec.europa.eu/digital-agenda/en/digital-europe

[64] European Union Agency for Network and Information Society (ENISA), "What does ENISA do?", European Union Agency for Network and Information Society Objectives, URL: https://www.enisa.europa.eu/about-enisa/activities

[65] European Cyber Security Protection Alliance (CYSPA), "Deliverable 2.2.1 – Impact contribution and approaches – European Policies and Directives". FP7-ICT-2011-8 / 318355, 01-10-2012, page 10

[66] European Cyber Security Protection Alliance (CYSPA), "Deliverable 2.2.1 – Impact contribution and approaches – European Policies and Directives". FP7-ICT-2011-8 / 318355, 01-10-2012, pages 9-14.

[67] Eg. N. Robinson et al., "Data and Security Breaches and Cyber-Security Strategies in the EU and its International Counterparts", pages 80/96, report IP/A/ITRE/NT/2013-5 PE 507.476 to the ITRE Committee of the European Parliament, September 2013. In: Axel Arnbak, "Any Colour You Like: the History (and Future?) of E.U. Communications Security Policy", IViR/Berkman Roundtable, July 2014.

[68] European Commission, "Communication on Cybersecurity Strategy of the European Union - An Open, Safe, and Secure Cyberspace", February 2013, URL: http://ec.europa.eu/digital-agenda/en/news/communication-cybersecurity-strategy-european-union-%E2%80%93-open-safe-and-secure-cyberspace

[69] European Commission, "Communication on Cybersecurity Strategy of the European Union - An Open, Safe, and Secure Cyberspace". URL: http://ec.europa.eu/digital-agenda/en/news/communication-cybersecurity-strategy-european-union-%E2%80%93-open-safe-and-secure-cyberspace

> "Currently, there is an impressive collection of directives, organisations, policies and the like, which makes it difficult to instantly and fully grasp how this broad topic is addressed within the EU. The fragmented and intransparent approach manifests itself in the EU CSS which is, despite its title, not (yet) able to singlehandedly take on the role a general European cyber security strategy as it lacks some essential aspects of what makes a strategy effective."[70]

This quote from the CYSPA report underlines that the EU Cybersecurity policy structure is fragmented and blurry. There are many independent actors involved in the EU's Cybersecurity policy, yet there is no single point of coordination or common understanding of what Cybersecurity exactly entails. Combined, these factors impede collective EU action and (according to Cox and McCubbins' criterion) decrease decisiveness. This is made worse by the fact that in the search for international cooperation Member States still act alone instead of from the EU block. How this bypasses, complicates, or even frustrates EU initiatives for cooperation, will be shown in the next section.

[70] European Cyber Security Protection Alliance (CYSPA), "Deliverable 2.2.1 – Impact contribution and approaches – European Policies and Directives". FP7-ICT-2011-8 / 318355, 01-10-2012, page 29.

Barrier 4: Bilateral Agreements

In the past few years, the EU has concluded several bilateral agreements on Cybersecurity issues with countries such as the US, China, Japan, Mexico and Brazil.[71] Although there is a need for external policy on Cybersecurity, the EU should first get is internal activities aligned, before starting negotiations with other (non-EU) countries. After all, the internal EU-coherence will influence the position in external affairs. As former president of the European Parliament Jerzy Buzek has stated: "The strength of the EU's external policy is determined by its internal cohesion".[72] Since the EU's Cybersecurity still has an Intergovernmental character, the current policy is focussed on national gain rather than EU coherence or cohesion.[73] This lack of internal EU cohesion is influencing the EU's external power – and thus its ability to make strong bilateral treaties. After all, how can the EU negotiate on Cybersecurity with external partners, if it can't even agree among itself on this issue?

James Andrew Lewis, director at the U.S. Center for Strategic and International Studies, has argued that bilateral agreements could be useful as a mechanism for Cybersecurity cooperation. [74] It is true that bilateral relationships offer a number of advantages. As Lewis claims, a state can enter into a relationship with individual states of its choosing, which permits it to regulate only those obligations it is willing to accept.[75] From an US point of view, Lewis argument is understandable: the US is a dominant party in any bilateral agreement, with a clear stance on Cybersecurity issues. Nonetheless, at this time, bilateral agreements are not a proper instrument for the EU. As stated, many actors are involved in the EU's Cybersecurity policy, and which actor takes up action depends on their interpretation of the term Cybersecurity. This leaves the EU vulnerable in discussing bilateral treaties: without a strong single point of view other major players such as the US, China or Japan (who do have a strong viewpoint) have the advantage in negotiations. It is likely that the EU will end up accepting standards brought up by the other party, just because there is no clear EU policy yet on certain points. Hence, only when the EU has its own stance clear on Cybersecurity issues, it can act as a strong and determined negotiator. This in turn will only happen when the EU organisation on Cybersecurity becomes less fragmented.

Another problem with bilateral treaties is based at the level of the Member State. These bilateral treaties could complicate the objectives of EU negotiations or EU policy as such. For example, The Netherlands and Italy recently held bilateral meetings with the US on Critical Infrastructure protection.[76] One could state that Italy and the Netherlands can be considered first movers, and that their agreements can be copied or scaled up to the European level in a later stage. However, in

---

[71] European Strategic Partnership Observatory (ESPO), Thomas Renard, "The Rise of Cyber-Diplomacy: the EU, its Strategic partners and Cyber-Security", Joint initiative of FRIDE and the Egmont Institute, Working Paper 7, June 2014. Page 12, URL: http://fride.org/download/WP7_The_rise_of_cyber_diplomacy.pdf

[72] Antoni Wierzejski, "Verheugen: EU needs to respond to external, internal chaos", EurActiv.com, 12 July 2013. URL: http://www.euractiv.com/global-europe/verheugen-eu-needs-respond-exter-news-529281

[73] Krzysztof F. Sliwinski, "Moving Beyond the European Union's Weakness as a Cyber-Security Agent", page 1.

[74] James Andrew Lewis, "Cyber Security: Turning National Solutions into International Cooperation", Significant Issues Series, Volume 25, Number 4, Center for Strategic and International Studies (CSIS), Washington, August 2003, Page 47-48.

[75] James Andrew Lewis, "Cyber Security: Turning National Solutions Into International Cooperation", 2003.

[76] Jody R. Westby, "International Guide To Cyber Security", American Bar Association, Privacy & Computer Crime Committee, Section of Science & Technology Law, 2004. Page 4.

reality such bilateral agreements hamper the EU external policy on two levels. Initially, the chances of achieving an EU agreement with the US *on this topic* of Critical Infrastructure Protection are diminished, as Member States have made their own arrangements. More important, the need to come to *a common EU policy on such topics* is also diminished, which complicates the formation of a EU external policy on Cybersecurity issues in general. When many of these (conflicting) bilateral treaties are set up, this will therefore undermine an EU policy as such. Member States will no longer feel the need for an EU policy, even if this would in fact improve their negotiation position. This is a lost opportunity, for the EU could ensure a strong block to negotiate on equal footing with other major powers, such as the US and China.

A third problem is one Lewis himself addresses as well: bilateral treaties are simply not suitable for Cybersecurity, as they involve only two players. Cybersecurity by definition only works with many players, for it is a global phenomenon. As Lewis himself states:

> "…bilateral relationships are best suited for matters that affect only the two signatory states rather than for problems that are **truly global** or even regional in nature."[77]

However, bilateral agreements can be useful in case of relationships between major power blocks, for this would still provide the global dimension Cybersecurity needs. This can merely work when the negotiators are equal, for example: a bilateral treaty between the US and EU, EU and China, or China and US. That way, the number of bilateral treaties can be reduced to a minimum: instead of 28 Member States signing bilateral treaties with the US, the EU would, as a single entity, negotiate one bilateral agreement. This is why it is necessary for the EU to convince its Member States to focus primarily on a common EU approach, thus ensuring that the EU will become a major Cybersecurity player. This would decrease the number of independent actors in the EU – and thus, in light of Cox and McCubbins definition, increase decisiveness.

[77] James Andrew Lewis, "Cyber Security: Turning National Solutions Into International Cooperation", Page 45.

Chapter Summary

To conclude, the EU's Cybersecurity approach and internal organisation is not optimal yet. Many barriers exist in the current Cybersecurity policy structure. First of all, sharing information on threats is currently a matter of 'quid pro quo'. To effectively deal with Cyberthreats, however, pro-active information sharing is necessary. Second of all, there is no common notion of what 'Cybersecurity' or 'Cyberattack' entails. Although this problem has been addressed by ENISA, no definition was provided in the recent EU Cyber Security Strategy. The effect is a blurry picture, in which it is unclear which institution should act in which case of Cybersecurity. "Triple division" is the result: division between EU and NATO, EU and Member States, between Member States, and within EU institutions. In the first case (EU-NATO), some division is inevitable, and current problems could be solved relatively easily with more coordination and a clear definition. The second and third case of fragmentation are more challenging. Currently, both the EU and Member States are managing Cybersecurity policy, which causes confusion about who should act in which case. This is especially true as Cybersecurity policies from Member States are not uniform. As a result, a coherent and thus decisive EU strategy cannot be set up. An EU wide definition is necessary to solve this problem.

Another problem is fragmentation between EU institutions. As there is no single point of coordination on Cybersecurity issues, several institutions have taken up topics in their area, creating a true patchwork. An opaque and complicated landscape is the outcome – it is extremely difficult to grasp who is responsible for which policy. Though the "Cyber Security Strategy of the European Union" was supposed to solve this issue, it failed to do so. Considering Cox and McCubbins, we can conclude that the four-levelled division results in a decrease in the EU's decisiveness on Cybersecurity issues.

An additional problem is found in bilateral treaties. The EU has recently concluded several bilateral agreements with major players. However, the EU should first align its internal activities, as internal coherence will influence their position in external affairs. James Andrew Lewis has argued that bilateral agreements can be useful for several reasons. Though his views are understandable from his American point of view, the situation is different for the EU. As there is no single point of coordination for Cybersecurity policy, the EU could be vulnerable in negotiations. The EU should first become less fragmented, before it can act as a strong and determined negotiator.

Also, bilateral agreements of Member States with non-EU countries hamper the EU's external Cybersecurity policy. The need for cooperation in the specific field of the agreement will be diminished for the specific state making the agreement. At the same time, if many Member States make such agreements, the need for a common EU policy on Cybersecurity topics at large is undermined. Member States will no longer feel the need for an EU policy, even if this would in fact improve their negotiation position. This is a lost opportunity, for the EU could ensure a strong block to negotiate on equal footing with other major powers, such as the US and China. Also, it would decrease the separation of powers in the EU – and thus, in light of Cox and McCubbins definition, increase decisiveness. Eventually, bilateral agreements are not suitable for a global phenomenon as Cybersecurity. There is however an exception: in case of major power blocks negotiating as equals, the number of bilateral treaties can be kept low and the global dimension could be sufficiently guaranteed.

Chapter 3
Comparison with the US: a more decisive policy?

> **"Coming together is a beginning, keeping together is progress and working together is success" - Henry Ford**

To ensure a strong Cybersecurity policy, "working together" is crucial. As Cybersecurity policy is such a young policy field, it is interesting to see how other major players have ensured a decisive policy. This chapter compares the structure of Europe's Cybersecurity policy with that of another major player: the United States. The US is a federation of states (in other words: supranational policy making) while Europe is still dealing with Cybersecurity through a system of cooperation. It is therefore interesting to see what the EU could achieve by getting Cybersecurity to the supranational level / community method. This chapter shortly analyses the benefits and drawbacks of the US Cybersecurity policy, by comparing it with the European policy. It will do so with the sub question: "What are the differences between the European and US Cybersecurity policy structure? Could and should the EU adopt certain parts of the US policy?"

The policy makers: DoD & DHS

In the US, there is a strict hierarchical structure on Cybersecurity policy. Two departments have main responsibility: the Department of Homeland Security (DHS) and the Department of Defense (DoD). Both have tasks in the area of Cybersecurity, but unlike in Europe there is much cooperation and alignment between the departments. Crucial in this is the 2010 Memorandum of Agreement, which outlines which department has which responsibility.[78] The document is extremely important, simply because it makes a distinction in responsibilities in the first place. Although other institutions (such as the NSA) are involved in US Cybersecurity policy, they only act under the management of the DoD and DHS. Thus, the number of actors involved in the Cybersecurity process is brought back to two. Remembering Cox and McCubbins' criteria, this will increase their decisiveness.

This does not mean that the EU has a different Cybersecurity policy content. Nearly all of the things the US does, have been done on the European level as well: establishing CERTs*, raising awareness, protection of Critical Infrastructure, etc. However, the speed and manner through which Cybersecurity policy is formed is different in the US: due to their federal (and hierarchic) structure the legislative process is a lot quicker.[79] Since the EU still deals with Cybersecurity on an intergovernmental (cooperative) level, their policy is slow and passive (as mentioned in chapter 2). In the US, however, an institution discovering an untreated topic can report this gap to DoD or DHS, after which it can quickly be translated into legislation. For example, if the NSA discovers a gap, it can report this to the DoD, which in turn will push the problem up towards legislative bodies. In the EU, this would not happen – if for example ENISA finds a gap, it would have no central point of coordination to report this to – instead, it will try to deal with it themselves, without knowing if other institutions have already done something on the matter. In this case, ENISA might make a call for legislation to the European Commission, but the chances of being heard are limited, as ENISA is only one of the many institutions, with its voice getting lost in the 'crowd'. Also, even if the Commission acknowledges the problem, it will need all 28 EU Member States to initiate action (table 3.2).

[78] Office of Security Review, "Memorandum of Agreement Between The Department of Homeland Security And The Department of Defense, Regarding Cybersecurity", Department of Defense, October 2010, URL: http://www.dhs.gov/xlibrary/assets/20101013-dod-dhs-cyber-moa.pdf

* CERTs, Computer Emergency Readiness Teams, are essential for Critical Information Infrastructure Protection. CERTS acts as a primary Security Service Provider for both Governments and Citizens. As ENISA states, they work like a fire brigade: they are the only ones which can react when a security incident occurs. It thus mostly acts as a reactive service: incident response.

[79] United States House of Representatives, "The Legislative Process", How Are Laws Made?, URL: http://www.house.gov/content/learn/legislative_process/

Separating and Coordinating: the common definition and Cybersecurity coordinator

In contrast to the EU, the US does have a common definition on what exactly Cybersecurity entails. In the National Security Presidential Directive 54 several definitions on cyber topics are given. In this document 'Cybersecurity' is defined as:

> "Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communication services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-repudiation"[80]

The document also gives definitions on what a Cyberattack, Cyberintrusion, Cyberexploitation or Cyberincident entails. The importance of these definitions should not be underestimated – by separating types of attacks determining who should act in which case becomes much easier. Each definition can be assigned to the party most suitable for it. These definitions from National Security Presidential Directive 54 are key, since they have been copied in other documents, such as the Memorandum of Agreement from 2010.[81] This shows general acceptance of the terms.

Furthermore, the US has a Cybersecurity Coordinator, Michael Daniel, whose position was created in 2009 by President Obama. Often referred to as the "Cyber Czar" [82], Daniel oversees the agencies implementation of the national Cybersecurity strategy and policy.[83] As he is also a special assistant to the President, issues can easily be passed to the executive branch. With this, the coordinator increases US decisiveness: the position further reduces the amount of policy levels, as it forms a bridge between the presidential office and the Departments of Defense and Homeland Security.

Together, the definitions, Memorandum of Agreement, and overseeing coordinator, ensure a coordinated approach. As mentioned in the previous chapter, the EU has a patchwork of institutions with various roles and responsibilities, which is mostly problematic, because there is no coordination between these institutions. The combination used in the US solves this problem, resulting in a much more coordinated policy than the one in the EU, as can clearly be seen in table 3.1 and table 3.2. DoD and DHS can align through looking at the definitions, and in case of doubt can deliberate with the Cybersecurity coordinator. With this, deciding who should act on which issue is made a lot

[80] U.S. Government "National Security Presidential Directive 54/Homeland Security Presidential Directive 23", DOCID: 4123697, The White House, Washington, 9 January 2008, URL: http://fas.org/irp/offdocs/nspd/nspd-54.pdf

[81] Office of Security Review, "Memorandum of Agreement Between The Department of Homeland Security And The Department of Defense, Regarding Cybersecurity", Department of Defense, October 2010, URL: http://www.dhs.gov/xlibrary/assets/20101013-dod-dhs-cyber-moa.pdf

[82] Robert M. Lee, "It Does Matter That The White House Cybersecurity Czar Lacks Technical Chops", Forbes, August 2014, URL: http://www.forbes.com/sites/frontline/2014/08/25/it-does-matter-that-the-white-house-cybersecurity-czar-lacks-technical-chops/

[83] White House Profile, "Michael Daniel: Special Assistant to the President and Cybersecurity Coordinator", The White House Blog, URL: https://www.whitehouse.gov/blog/author/Michael%20Daniel

easier. For the EU, establishing a Cybersecurity coordinator could greatly help the Cybersecurity Policy: it would help create a single point of coordination and overview. However, it should be noted that the creation of a Cybersecurity coordinator alone is not enough. It should be accompanied by a reduction of institutions involved, so that the number of actors would be manageable to the coordinator.

Table 3.1, situation in the United States

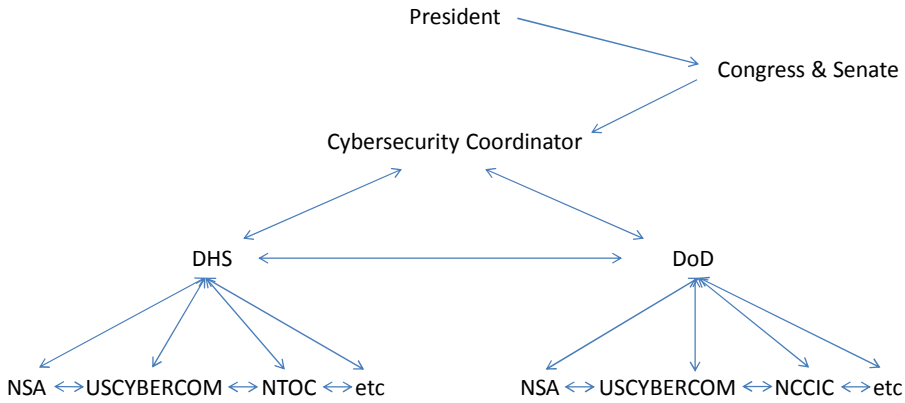
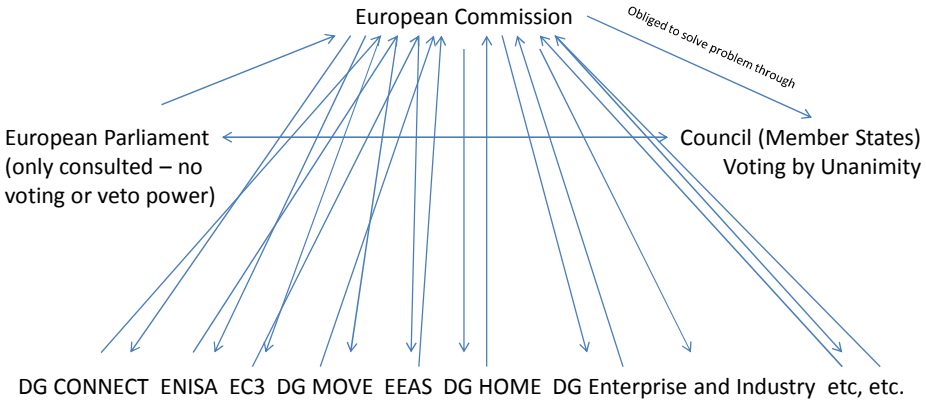


Table 3.2, situation in the European Union



*

[*] Reading the digital version? Click the picture to view the process step by step.

The EU's secret weapon?

In Cox and McCubbins' definition, policy decisiveness includes "the ability to decide or pursue a consistent policy".[84] Regarding this consistency of policy the EU has a big advantage over the US. As the EU is not a federal government, established policies won't be easily changed: this would again require all 28 Member States to reach consensus. An example are the sanctions on Russia in dealing with the Ukraine crisis: the EU countries were quick to decide on these sanctions, but now that France and Germany have concerns about the effectiveness of the sanctions, turning them back is not that easy.[85] [86] In the US, however, policies established by one government could be changed by the next government: all that is required, is a majority of the Congress and Senate vote in favour of them. The examples here are numerous: policies regarding Afghanistan, the Patriot Act, Guantanamo Buy, the "No Child Left Behind Act"[87], and funded research on embryonic stem cells, are all examples of what President Obama has changed since his predecessor Bush has left the office.

However, in the field of Cybersecurity, this "consistency of policy" advantage for the EU is disproportionate to the advantages policy making in the US offers. The negotiating process between EU Member States only results in an outcome acceptable to all parties, instead of an outcome that is unacceptable to some Member States, but forced upon them through QMV voting. In the last case more can be achieved, while in the first case the outcome will only reflect the lowest-common-denominator. To accelerate progress in the Cybersecurity field, the EU decision making procedure should therefore be set to Qualified Majority Voting - even if this means that the outcome won't always satisfy all parties. However, as there has never been an initial decision to place classic Foreign and Security policy under the authority of central EU institutions, there is also no pressure to extend the authority of institutions to Cybersecurity policy. In other words, there is no spill-over effect to get Cybersecurity to the community method. This again confirms the Intergovernmentalism notion that Member States, not the EU institutions, are the main actors in European Integration in this area. The clear result has been mentioned before: EU policy making in Cybersecurity is slow and lags developments, while the US can respond to incidents much quicker.

Considering all the criteria of Cox and McCubbins, the US therefore scores much better on Cybersecurity policy decisiveness: powers are less separated and less independent actors are involved in the political bargaining process. In the US, policies can quickly be adapted to new situations – which is something Cybersecurity, with its fast evolving character, requires. The only

---

[84] Definition of Cox & McCubbins as stated in Kyung Joon Han, "Policy decisiveness and responses to speculative attacks in developed countries", European Journal of Political Research, Volume 48, Number 6, 2009, pages 723-755, page 730. URL: http://onlinelibrary.wiley.com.ezproxy.leidenuniv.nl:2048/doi/10.1111/j.1475-6765.2009.01835.x/epdf

[85] Danny Vinik, "Why Germany Doesn't Want Sanctions Against Russia, in Two Charts", The New Republic, 3 March 2014. URL: http://www.newrepublic.com/article/116836/why-germany-doesnt-want-sanction-russia-invading-ukraine

[86] Hans Kundnani, "Leaving the West Behind – Germany looks east", Foreign Affairs Magazine, January/Februari 2015 issue, Published by the Council on Foreign Relations, URL: https://www.foreignaffairs.com/articles/western-europe/leaving-west-behind

[87] The White House, "Reforming No Child Left Behind", Education, 2015, see also URL: https://www.whitehouse.gov/issues/education/k-12/reforming-no-child-left-behind

way the EU could achieve this too, is by placing Cybersecurity under the Qualified Majority Voting, thus speeding up the decision making process. Comparing the EU and US Cybersecurity policies in light of Henry Ford's quote, the EU is still beginning to "come together", while the US is already "working together".

Chapter Summary

In the United States, Cybersecurity policies are arranged through a strict structure. The Department of Homeland Security (DHS) and Department of Defense (DoD) are the main responsible parties. Making a distinction in who takes up which part of Cybersecurity is easier in the US, as the US has common definitions on what Cybersecurity, Cyberattack, Cyberintrustion, etc, entails. To help coordinate tasks, the position of Cybersecurity Coordinator was created in 2009. Furthermore, a Memorandum of Agreement between DoD and DHS was signed in 2010. Together, these three factors ensure a highly coordinated policy.

One could argue that the EU has the benefit of consistency in its Cybersecurity policies. As 28 Member States are involved in the decision making process, policies established won't be easily changed. Although this is true, the advantage is disproportionate compared to those of the US – the US has less independent actors and less separation of powers. This makes the US highly decisive according to Cox and McCubbins. The structure ensures that policies can quickly be adapted to new situations, which is exactly what Cybersecurity (with its fast evolving character) requires. Comparing the EU and US Cybersecurity policies in light of Henry Ford's quote, the EU is still beginning to "come together", while the US is already "Working Together".

To increase policy decisiveness, the EU could benefit from the instalment of a similar Cybersecurity Coordinator, who would overlook which EU institution does what. This should be accompanied by a reduction in the number of institutions involved. Although this helps coordination, it does not help create a faster policy environment. To achieve this, EU Member States should let go of the idea that national control is best and place Cybersecurity under the Qualified Majority Voting procedure. Only then the EU can be quick, adaptive, and decisive.

Conclusion:

Posting pictures on Facebook, sending messages through Gmail, or transferring money using a bank account application – these days, technological possibilities seem to be endless. Cyberspace has become a vital part of both our lives and our society; but not all that glitters is gold. In recent years major Cyberthreats have come up, which are occurring more often and are getting technologically more advanced. A decisive Cybersecurity policy is necessary to protect civilians from the dangers that digitalization brings. For Europe, a logical way to arrange this would be in the EU framework. However, EU Member States have not given up their national policies regarding Cybersecurity yet. Currently, Cybersecurity legislation is issued from both the Member State and the European level. This is typical for the EU's central question: how can European Integration be explained best and what this will mean for the EU's future? While Neo-Functionalism theory states that integration is self-sustaining, Intergovernmentalism argues that states (national governments) are the main actors in the EU's integration process. In this thesis Cybersecurity was analysed as part of the central debate: the clash between decision making on the national and EU level is specifically problematic in the (borderless) case of Cyberspace. As Europe has received much criticism on its Cybersecurity policy, one could wonder whether this policy is in fact decisive. An effort was therefore made to analyse this, with the main question: "To what extent is Europe decisive in its Cybersecurity policy?".

To answer the main question, it was first of all important to define the term 'Cybersecurity'. The choice was made to interpret the word in the broadest sense possible: it includes any form of protection against any sort of Cyberattack. On a scale of impact, it is thus not limited to a single citizens' privacy (on the lowest level), nor to Cyberwarfare (on the highest level). Protection against Cyberbullying, Cybercrime, Cyberterrorism and Cyberwarfare therefore all fall under the umbrella of Cybersecurity.

Secondly, several criteria for decisiveness were set up. This was done by applying Cox and McCubbins definition of "policy decisiveness" to the EU. Cox and McCubbins argue separation of power will lead to indecisiveness. Also, independent actors in the political bargaining process make it harder to maintain collective action.[88] I.e., the more actors, the more indecisive the EU will be. The definition of Cox and McCubbins was augmented with the criteria "policy speed", since rapid developments in Cyberspace ask for quick policy adaption to these developments.

Finally, three sub questions were set up. The first sub question was: "Have certain 'watershed' moments influenced Europe's Cybersecurity policy? If so, in what way?". The second sub question was: "What barriers exist in this current policy structure?". The third sub question was "What are the differences between the European and US Cybersecurity policy structure? Could and should the EU adopt certain parts of the US policy?".

[88] Definition of Cox & McCubbins as stated in Kyung Joon Han, "Policy decisiveness and responses to speculative attacks in developed countries", European Journal of Political Research, Volume 48, Number 6, 2009, pages 723-755, specifically page 730. URL: http://onlinelibrary.wiley.com.ezproxy.leidenuniv.nl:2048/doi/10.1111/j.1475-6765.2009.01835.x/epdf

In answering the first sub question, “Have certain watershed moments influenced the European Cybersecurity Policy? If so, in what way?”, it became clear that several watershed moments have had influence on the European Cybersecurity policy - yet this is has not always helped decisiveness. The first watershed moment that was analysed was the Commission proposal from 1990, which suggested that Information Security should be set to the EU level, as information security was part of the internal market. The proposal suggests that the ordinary legislative procedure should be applied. However, the Council of Ministers, representing the national governments, were not convinced that they should give up their national sovereignty in this field. This was a crucial moment in Cybersecurity history, as the changes to the original text ensured that the Commission had no power over Cybersecurity policies. Thus, the further course of Cybersecurity policy would be in the hands of the Member States: in other words, power in this area was separated into 28 pieces.

A second watershed moment came in 2001, when the European Commission put forward a proposal that implemented several of the ideas of a Cybercrime convention. Although the idea of Cybercrime legislation at the EU level was confirmed, the idea of placing this under Commission competence was not: major points were once again excluded from Commission competence, as they touched too closely upon the exclusive area of National Security.

The third watershed moment came in 2007, when Estonia was the target of a major DDOS attack. Here, Europe’s Cybersecurity policy was influenced to some extent, as Estonia proved to be a wake-up call for both EU and NATO. However, while NATO’s quickly adapted its policy, the EU’s policy implications were slow and limited. It took the EU two years to come up with solutions, and when these came, they mostly included new legislation, rather than an actual shift in decision making. Policies stayed on the intergovernmental level.

A fourth watershed moment was Stuxnet in 2010. Stuxnet became the first Cyberweapon in history to cause physical damage. Although Stuxnet initially shocked Europe, the classic paradox from Estonia resurfaced: it created more awareness, but Member States still held onto national control.

Thus, the main actors proved to be the Member States: from the very start, national leaders viewed Cybersecurity as part of their national security strategies. Although international cooperation was sought more often after Estonia and Stuxnet, the national character of Cybersecurity was sustained.

In answering the second sub question, “What barriers exist in this current policy structure”, it became clear that the current Cybersecurity policy landscape is as opaque and fragmented. There is no common definition on what the term “Cybersecurity” or “Cyberattack” entails, which makes it hard to decide who should act in which case. The result is division on three levels: EU-NATO, EU-MS, and between EU-institutions. In the first case, division of politics is logical – more attention could be given to who takes up what, but no major problems occur here. The division between EU and Member States is problematic: as both the EU and Member States manage Cybersecurity policy, confusion about who should act in which case is caused. This is especially true as Cybersecurity policies from Member States are not uniform. As a result, a coherent and thus decisive EU strategy cannot be set up. An EU wide definition is necessary to solve this problem. The last case of division, between EU-institutions, is especially problematic: many EU-institutions have taken up Cybersecurity

in their area of expertise, but since there is no single point of coordination, no one knows who exactly does what. The result is patchwork of institutions, without strong management.

The problem of division is made worse by the fact that Member States conclude separate bilateral treaties. These agreements hamper the EU's external Cybersecurity policy, as the need for cooperation in the specific field of the agreement will be diminished. At the same time, the overall need for a common EU policy on Cybersecurity topics will be undermined. For the EU, bilateral agreements are not a suitable instrument for Cybersecurity either: Europe should first align its internal activities, as this will ensure a stronger position in external affairs.

In answering the third sub question, "What are the differences between the European and US Cybersecurity policy structure? Could and should the EU adopt certain parts of the US policy?", it was clear that some major differences exist between the EU and US Cybersecurity policy structure. In the US, Cybersecurity is arranged in a strict structure, with the Department of Homeland Security (DHS) and Department of Defence (DoD) being the main actors. Due to a common definition, a Cybersecurity Coordinator with a direct link to the President, and a Memorandum of Agreement between DHS and DoD, a highly coordinated policy is ensured. However, the EU does have the advantage of consistency of policies. As all EU Member States have veto powers in the decision making process, policies established won't be easily changed – this would again require consensus among 28 Member States. Nonetheless, this advantage is disproportionate to those the US has in Cybersecurity policy making. The US has less independent actors, less separation of power, and a higher policy speed, making it a highly decisive Cybersecurity player. The US structure ensures that Cybersecurity policies can quickly be adapted to new situations – which is exactly what a fast evolving phenomenon such as Cybersecurity requires.

In concluding the main research question, "To what extent is Europe decisive in its Cybersecurity policy?", the answer can thus be that although the topic of Cybersecurity has been addressed in the EU, the European Cybersecurity policy is not that decisive yet. In analysing the three criteria of decisiveness, we can see that the "separation of powers" is large. Europe is still dealing with Cybersecurity on the intergovernmental level. Thus, all 28 Member States share power – in other words, power is separated into 28 pieces, rather than merged into one piece: a single EU power.

Concerning the "amount of independent actors", Europe is once again performing poorly. The amount of independent actors is huge: as there is no common definition, division on three levels has come up: EU-NATO, EU-MS, and between EU institutions. The EU-MS division and fragmentation between EU institutions is especially problematic here. Currently, too many actors seem to be involved in the Cybersecurity policy process. There is no single point of coordination, and only little willingness to share information on Cyberthreats. Bilateral agreements further split the EU. Combined, these factors influence Europe's Cybersecurity policy decisiveness immensely: it makes the EU a less decisive player.

The EU also has a disadvantage in the third criterion of “policy speed”. Since the EU is still dealing with Cybersecurity from the Member State level, the policy making process is slow and passive. It requires all 28 Member States to reach consensus.

In light of the broader debate of how European Integration can best be explained, and what this means for the future of the EU, it thus is clear that the theory of Intergovernmentalism best explains the history of Europe’s Cybersecurity policy. The national approach has prevailed throughout: Member States are still the main drivers in the integration seat of this policy area. Although developments such as Estonia and Stuxnet have accelerated (pending) legislation, this can mainly be attributed to a temporary convergence of governmental preferences, rather than to an actual mentality switch to supranational decision making.

Intergovernmentalism theory can furthermore be confirmed by the fact that there is no “spill-over” effect to the area of Cybersecurity. As classical security policy is also still in the intergovernmental decision making process, there are no created institutions to drive Cybersecurity forward. However, to increase decisiveness in the future, a more Neo-Functionalist approach would be best. The internet challenges traditional Westphalia notion of sovereignty: thinking in state terms will no longer suffice. Yet not all is lost for the EU. To increase European decisiveness in Cybersecurity policy, several things could be done.

First of all, the EU could benefit from the instalment of a Cybersecurity Coordinator similar to the one the US has. This coordinator could then overlook which EU institution does what. The lack of a single point of coordination would thus be solved. However, the instalment of such a coordinator should be accompanied by a reduction of the number of institutions involved in the EU’s Cybersecurity policy. How exactly this could be done, is an interesting topic for further research. Furthermore, a common EU definition on terms such as “Cybersecurity”, “Cyberattack”, “Cyberwarfare”, “Cyberintrusion”, “Cybercrime”, “Cyberexploitation”, etc., etc. should be set up. The lack of such a definition results in enormous problems, as can be seen in the previous chapters. Besides these improvements in coordination, the EU should create a faster decision making process for its Cybersecurity policy. To achieve this, the EU Member States should let go of the idea that Cybersecurity is a matter of national safety, and place Cybersecurity under the Community Method (Qualified Majority Voting procedure). Only then, the EU will be a quick, adaptive, and decisive Cybersecurity player.

Bibliography

A

Andrew Moravcsik, “In Defence of the Democratic Deficit: Reassessing Legitimacy in the European Union”, Center for European Studies, Working Paper No. 92, Journal of Common Market Studies, Volume 40, Issue 04, 2002, pages 603-624. URL: http://aei.pitt.edu/9136/1/Moravcsik92.pdf

Antoni Wierzejski, “Verheugen: EU needs to respond to external, internal chaos”, EurActiv.com, 12 July 2013. URL: http://www.euractiv.com/global-europe/verheugen-eu-needs-respond-exter-news-529281

Axel Arnbak, “Any Colour You Like: the History (and Future?) of E.U. Communications Security Policy”, IViR/Berkman Roundtable, 18 April 2014, page 4, 18, .

B

Bouwman and Marácz “Nederland moet inzetten op international cybersamenwerking”, Atlantisch Perspectief, Number 6, 2012, pages 22-27. URL: http://www.atlcom.nl/ap_archive/pdf/AP%202012%20nr.%206/Bouwman%20en%20Maracz.pdf

Bruce Schneier, “The Story Behind The Stuxnet Virus”, Forbes, 07 October 2010, URL: http://www.forbes.com/2010/10/06/iran-nuclear-computer-technology-security-stuxnet-worm.html

C

CEN / CENELEC, “European Standardization: Cybersecurity” , CEN-CENELEC Sectors: Defence, Security and Privacy – Security. URL: http://www.cencenelec.eu/standards/Sectors/DefenceSecurityPrivacy/Security/Pages/Cybersecurity.aspx

COM(90) 314 final, OJ C 277/18, 5 November 1990, page 18 - in Axel Arnbak, “Any Colour You Like: the History (and Future?) of E.U. Communications Security Policy”, IViR/Berkman Roundtable, 18 April 2014, page 4

Commission of the European Communities, “Commission Communication on the Protection of Individuals in relation to the processing of personal data in the Community and Information

Security", COM(90) 314 final – SYN 287 and 288, Brussels, 13 September 1990, URL: http://aei.pitt.edu/3768/1/3768.pdf

Commission of the European Communities, 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", Brussels, 06 June 2001, COM(2001) 298 final, page 9

Consolidated Version of the Treaty on the Functioning of the European Union (TFEU) Article 68, in: Nigel Foster, "Blackstone's EU Treaties & Legislation 2014-2015", Oxford University Press, 25th Revised edition, August 2014.

Council Decision 92/242/EEC, in the field of security of information systems, Annex - Summary of action lines, Official Journal of the European Communities, 31 March 1992. URL: http://policy.mofcom.gov.cn/english/flaw!fetch.action?id=056235c9-75d6-4070-9a78-ab605e3ae84c

Cox & McCubbins, in Kyung Joon Han, "Policy decisiveness and responses to speculative attacks in developed countries", European Journal of Political Research, Volume 48, Number 6, 2009, pages 723-755, specifically page 730. URL: http://onlinelibrary.wiley.com.ezproxy.leidenuniv.nl:2048/doi/10.1111/j.1475-6765.2009.01835.x/epdf

D

Danny Vinik, "Why Germany Doesn't Want Sanctions Against Russia, in Two Charts", The New Republic, 3 March 2014. URL: http://www.newrepublic.com/article/116836/why-germany-doesnt-want-sanction-russia-invading-ukraine

E

Erki Kodar, "Applying the Law of Armed Conflict to Cyber Attacks: From the Martens Clause to Additional Protocol", ENDC Proceedings, Volume 15, 2012, pages 107–132. URL: http://www.ksk.edu.ee/wp-content/uploads/2012/12/KVUOA_Toimetised_15_5_Kodar.pdf

Europa, Synthèses de la législation, Glossary, "Open Method of Coordination", URL: http://europa.eu/legislation_summaries/glossary/open_method_coordination_en.htm

European Commission (E.COM) and High Representative of the European Union for Foreign Affairs and Security Policy (HR), Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "Cybersecurity

Strategy of the European Union: An Open, Safe and Secure Cyberspace". Brussels, 07-02-2013. JOIN (2013) 1 Final.

European Commission, "Communication on Cybersecurity Strategy of the European Union - An Open, Safe, and Secure Cyberspace", February 2013, URL: http://ec.europa.eu/digital-agenda/en/news/communication-cybersecurity-strategy-european-union-%E2%80%93-open-safe-and-secure-cyberspace

European Commission (E.COM) Communication to the European Parliament, Council, European Economic and Social Committee and the Committee of the Regions, "Protection Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience", Brussels, 30 March 2009, COM(2009) 149 final. URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF

European Commission (E.COM), "Digital Agenda for Europe", Digital Agenda for Europe - A Europe 2020 Initiative, URL: http://ec.europa.eu/digital-agenda/en/digital-europe

European Commission (E.COM) 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". Brussels, 07-02-2013. (COM)2013, 48 Final.

European Cyber Security Protection Alliance (CYSPA), "D2.2.1 – Impact contribution and approaches – European Policies and directives", Project Number FP7-ICT-2011-8 / 318355. 31 December 2013.

European Parliament Briefing "Cyber Defence in the EU: Preparing for Cyber Warfare?", European Parliamentary Research Service (EPRS), October 2014. URL: http://epthinktank.eu/2014/10/31/cyber-defence-in-the-eu-preparing-for-cyber-warfare/.

European Strategic Partnership Observatory (ESPO), Thomas Renard, "The Rise of Cyber-Diplomacy: the EU, its Strategic partners and Cyber-Security", Joint initiative of FRIDE and the Egmont Institute, Working Paper 7, June 2014. Page 12, URL: http://fride.org/download/WP7_The_rise_of_cyber_diplomacy.pdf

European Union Agency for Network and Information Society (ENISA), "EU Agency analysis of 'Stuxnet' malware: a paradigm shift in threats and Critical Information Infrastructure Protection" Press Release ENISA, 7 Oct 2010. URL: https://www.enisa.europa.eu/media/press-releases/eu-agency-analysis-of-2018stuxnet2019-malware-a-paradigm-shift-in-threats-and-critical-information-infrastructure-protection-1

European Union Agency for Network and Information Society (ENISA), "National Cyber Security Strategies in the World", ENISA National Cyber Security Strategies, URL: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world

European Union Agency for Network and Information Society (ENISA), “What does ENISA do?”, European Union Agency for Network and Information Society Objectives, URL: https://www.enisa.europa.eu/about-enisa/activities

European Union Committee of the Regions, “Digital Agenda For Europe, the role of regions and cities”, Background note Conference of the Committee of the Regions, Brussels, 2 July 2013, page 5. URL: http://cor.europa.eu/en/news/events/Documents/digital_agenda_background.pdf

Europol, “The Internet Organised Crime Threat Assessment (iOCTA) 2014”, European Cybercrime Center EC3 Europol, European Police Office, 2014. Page 14. URL: https://www.europol.europa.eu/ec3

H

H.A.M. Luijf et al., “Cross-Sector Information Sharing”, TNO 2014 R10945, TNO Rapport for the Dutch Ministry of Security and Justice, Project Number 032 32715, June 2014, Page 25.

Hans Kundnani, “Leaving the West Behind – Germany looks east”, Foreign Affairs Magazine, January/Februari 2015 issue, Published by the Council on Foreign Relations, URL: https://www.foreignaffairs.com/articles/western-europe/leaving-west-behind

I

Ian Traynor, “Russia accused of unleashing cyberwar to disable Estonia”, the Guardian, World News, Brussels, 17 May 2007, URL: http://www.theguardian.com/world/2007/may/17/topstories3.russia

J

Jack Clark, “Stuxnet threat rings EU alarm bells”, ZDNet, October 2010, URL: http://www.zdnet.com/article/stuxnet-threat-rings-eu-alarm-bells/

James Andrew Lewis, “Cyber Security: Turning National Solutions into International Cooperation”, Significant Issues Series, Volume 25, Number 4, Center for Strategic and International Studies (CSIS), Washington, August 2003, Page 47-48.

Jared Brow, “The Need for Greater Transatlantic Cybersecurity Cooperation”, Blog on Issues of International and European Security, ISIS Europe, 19 June 2014, URL: https://isiseurope.wordpress.com/2014/06/19/the-need-for-greater-transatlantic-cybersecurity-cooperation/

Jeremy Richardson and Sonia Mazey, “European Union: Power and Policy-making”, Routledge, Fourth Edition, 2015, page 40. URL: https://books.google.nl/books?id=l0ihBgAAQBAJ&pg=PA39&lpg=PA39&dq=intergovernmentalism+ir&source=bl&ots=E7Zkz3oj4t&sig=hoCZAZTCoGnsO029gfx09M1gm-Q&hl=nl&sa=X&ei=X8MwVZjuBtHraq6ugMAC&ved=0CDcQ6AEwAg#v=onepage&q=intergovernmentalism%20ir&f=false

Jody R. Westby, “International Guide To Cyber Security”, American Bar Association, Privacy & Computer Crime Committee, Section of Science & Technology Law, 2004. Page 4.

Josh Halliday, “Stuxnet worm is the ‘work of a national government agency’”, The Guardian, 24 September 2010, URL: http://www.theguardian.com/technology/2010/sep/24/stuxnet-worm-national-agency

Joshua McGee, “NATO and Cyber Defense: A Brief Overview and Recent Events”, Center for Strategic and International Studies (CSIS), 8 July 2011, URL: http://csis.org/blog/nato-and-cyber-defense-brief-overview-and-recent-events

K

Kenneth Geers, Darien Kindlund, Ned Moran, Rob Rachwald, “World War C :Understanding Nation-State Motives Behind Today’s Advanced Cyber Attacks”, FireEye, September 2013, URL: http://www.fireeye.com/resources/pdfs/fireeye-wwc-report.pdf

Kertu Ruus, “Cyber War I, Estonia Attacked from Russia”, The European Institute, published in: European Affairs, Volume 9, Issue 1-2, Winter/Spring 2008. URL: http://www.europeaninstitute.org/index.php/component/content/article?id=67:cyber-war-i-estonia-attacked-from-russia

Kim Zetter, “An Unprecedented Look At Stuxnet, The World’s First Digital Weapon”, Wired, 11 March 2014, URL: http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

Krzysztof Feliks Sliwinski, “Moving Beyond the European Union’s weakness as a Cyber-Security Agent”. Contemporary Security Policy, Volume 35, Nr 3, 2014. Pages 468-486. URL: http://www.tandfonline.com/doi/abs/10.1080/13523260.2014.959261?journalCode=fcsp20#.VYqnxU3759A

L

Leroy Hood, American Scientist, Born 10 October 1938, on Brainy Quote. URL: http://www.brainyquote.com/quotes/quotes/l/leroyhood652754.html

N

Nicole Falessi et al., “National Cyber Security Strategies: An Implementation Guide”, European Union Agency for Network and Information Security (ENISA), December 2012, URL: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-an-implementation-guide

North Atlantic Treaty Organization (NATO), “The North Atlantic Treaty”, Washington D.C., 4 April 1949, URL http://www.nato.int/cps/en/natolive/official_texts_17120.htm

N. Robinson et al., “Data and Security Breaches and Cyber-Security Strategies in the EU and its International Counterparts”, pages 80/96, report IP/A/ITRE/NT/2013-5 PE 507.476 to the ITRE Committee of the European Parliament, September 2013. In: Axel Arnbak, “Any Colour You Like: the History (and Future?) of E.U. Communications Security Policy”, IViR/Berkman Roundtable, July 2014.

O

Office of Security Review, “Memorandum of Agreement Between The Department of Homeland Security And The Department of Defense, Regarding Cybersecurity”, Department of Defense, October 2010, URL: http://www.dhs.gov/xlibrary/assets/20101013-dod-dhs-cyber-moa.pdf

P

Pippa Norris, “Digital Divide: Civic Engagement, Information Poverty, and the Internet Worldwide”, Cambridge University Press, 24 September 2001, page 47, figure 3.1: The Percentage of the Population Online by Major Region in 2000.

Portal European Commission, Digital Agenda for Europe, Cybersecurity and Privacy - Cybersecurity. Available at: http://ec.europa.eu/digital-agenda/en/cybersecurity

R

Ralf Bendrath & Florian Walther, “ The EU approach to Cybersecurity and Cybercrime: From the Virtual Schengen Border to Criminalising Hacker Devices”, Sigint Conference 2012 (May 2012).

Robert M. Lee, “It Does Matter That The White House Cybersecurity Czar Lacks Technical Chops”, Forbes, August 2014, URL: http://www.forbes.com/sites/frontline/2014/08/25/it-does-matter-that-the-white-house-cybersecurity-czar-lacks-technical-chops/

S

Scheherazade S. Rehman, “Estonia’s Lessons in Cyberwarfare”, USNews.com, 14 January 2013, URL: http://www.usnews.com/opinion/blogs/world-report/2013/01/14/estonia-shows-how-to-build-a-defense-against-cyberwarfare

Stephen Herzog, “Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses”, Journal of Strategic Security, Volume 4, Number 2: Strategic Security in the Cyber Age, Summer 2011, page 55. URL: http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1105&context=jss

T

The White House, “Reforming No Child Left Behind”, Education, 2015, URL: https://www.whitehouse.gov/issues/education/k-12/reforming-no-child-left-behind

U

United States House of Representatives, “The Legislative Process”, How Are Laws Made?, URL: http://www.house.gov/content/learn/legislative_process/

U.S. Government “National Security Presidential Directive 54/Homeland Security Presidential Directive 23”, DOCID: 4123697, The White House, Washington, 9 January 2008, URL: http://fas.org/irp/offdocs/nspd/nspd-54.pdf

W

White House Profile, “Michael Daniel: Special Assistant to the President and Cybersecurity Coordinator”, The White House Blog, URL: https://www.whitehouse.gov/blog/author/Michael%20Daniel

Wilbert de Vries, “Aanval op Mastercard.com werd vanuit Nederland opgezet”, Tweakers, 8 december 2010, URL: http://tweakers.net/nieuws/71230/ddos-aanval-op-mastercard-punt-com-werd-vanuit-nederland-opgezet.html

William J. Broad, John Markoff and David E. Sangerjan, “Israeli Test on Worm Called Crucial in Iran Nuclear Delay”, New York Times, 15 January 2011, URL: http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=0

Wolfgang Röhrig, “Viewpoints: Cyber Security and Cyber Defence in the European Union”, European Defence Agency (EDA), EDA Info Hub, Opinion. Brussels, 11 June 2014, URL: https://www.eda.europa.eu/info-hub/opinion/2014/06/11/viewpoints-cyber-security-and-cyber-defence-in-the-european-union

Y

YanTian and Concetta Stewart, “History of E-Commerce”, in: Mehdi Khosrow-Pour, “Encyclopedia of E-Commerce, E-Government and Mobile Commerce”, IGI Global, 2006, page 560.