Cyber security in the Context of European Integration – a New Beacon of National Acting inside the EU

By Fabian Hönicke (399241/s1369628)
Supervisors:
Prof. Dr. Markus Lederer
Prof. Dr. Marcel Boogers

Source: http://northrupcorporation.com/wpcontent/uploads/2014/03/iStock_000028716526_Medium.jpg

Table of Content

"We worried for decades about WMDs – Weapons of Mass Destruction. Now it is time to worry about a new kind of WMDs – Weapons of Mass Disruption."

Introduction

John Mariotti's words point towards the sheer insurmountable capabilities of the internet to throw over any kind of order in networks connected to it. Jörg Ziercke, president of the German Federal Office of Criminal Investigation (BKA) for example called cybercrime a new dimension of crime, being limitless in its potential to grow and cause damages (2013, p. 2). He further underlines that cybercrime relies on a small amount of resources, works across borders, and allows for the disguise of real and digital identities (Ibid.). These observations are completely in line with Sandro Gaycken's point of view, who states that any physical traces left for criminologists are often either eradicated, or simply rewritten in a distracting manner, leading to false locations and identities (2012, pp. 56-57). Moreover, the prospects of a successful attack increase with the complexity of the targeted system (Ibid. p.47). These rules ultimately apply to both, criminal and even military usage of cyber-related tools. Furthermore, John Arquilla (2013) asserts that "[…] it has grown ever more difficult to deny cyberwar's existence […]", which he bases on the fact that "[…] sustained cyberspace-based attacks were mounted against Estonia in 2007, and that the Russian ground invasion of Georgia in 2008 was accompanied by skilful hacker attacks on key military and governmental command and control sites […]" (p.81). The importance of communication systems has ever been recognized and related to nation states. Stephen D. Krasner (1991) already analysed the impact of power in communication and the allocation in terms of the pareto-principle over 20 years ago.

In this situation, Resolution 57/239[1] of the UN General Assembly calls for a common culture of cyber security. Yet, the term cyber security itself is often only vaguely described, leaving room for interpretation. Based on former research, it can for example be said that until today, no common or comprehensive framework has been established for a clear differentiation in terms of cyberwar (Fabian Hönicke, 2014)

The European Union as a successful example for peaceful and long-lasting integration, is assumed to potentially act as a role-model in merging the efforts of a common and constructive cyber security approach. Puzzling however is that national efforts to increase individual security measures still seem to be predominant, even though the internet as a tool intuitively contradicts the idea of acting without a strong and tight network of international partners. Exactly at this point lies the main interest of this paper. It will give answers to the question of *"How European cyber strategic efforts are conducted and by what logics they are consequently characterized"*. The accentuation of *European* is important, however the logics of globalisation, especially in terms of cyberspace, demand to go beyond European borders. Thus, bi- and multilateral agreements, as well as non-European actions influencing the European strategies will be taken into consideration. Nevertheless, the stance of EU Member States towards deepened European integration is focused.

In order to accomplish this task, two strands of intergovernmentalism will be displayed and used to analyse the cyber strategic behaviour of three EU Member States, being France, The UK, and Germany. These states have deliberately been chosen, as they are among the largest and most influential members of the European Union. Additionally, all three have a partly common, and at the same time unique history in European and World politics. Their interests in general security matters have been explained and analysed repeatedly (see Alexandra Jonas & Nicolai von Ondarza, 2010; Udo Diedrichs,

[1] Source: http://www.itu.int/ITU-D/cyb/cyber security/docs/UN_resolution_57_239.pdf

2012). Doing the same for cyber security efforts, thus seems to be a viable path. The two theoretical strands are embodied by the neo realist approach of Joseph M. Grieco, and Andrew Moravscik's liberal intergovernmentalist approach. This choice implies a comparatively pessimistic view on world politics when mirrored against liberal theories in a broader sense, and stresses the importance of nation states. Although there are authors declining the existence of decisive cyber threats and cyberwar, those believing in the latter being a danger to nation states, claim that it "[…] is global […] skips the battlefield […] [and] has begun" (Richard A. Clarke & Robert K. Knake, 2010, 31). With intergovernmentalism naturally being interested in the fate of nation states, Joseph M. Grieco and Andrew Moravscik and their respective theories have been logical choices in this matter.

Consequently, the first section introduces both theories, and will deliver an in-depth answer to the question, why two intergovernmentalist theories have been picked for the purpose of this paper. In addition, the hypotheses related to the research question are subsequently constructed and their specific requirements displayed as well. The second section summarises the cyber strategic capabilities, goals, and efforts of France, the UK, and Germany. First resemblances, as well as differences between them are exposed here as well. The third section portrays EU-wide and global actions and plans concerning cyber strategic efforts. These include bilateral, as well as multilateral treaties, agreements, and non de jure cooperation. In the fourth section, the EUs' and its Member States' cyber strategic efforts are interconnected with the proposed hypotheses. They are evaluated on the basis of the two chosen theories, whereby national efforts are brought in line with the existing agreements and treaties. Finally, the last section pictures potentials, barriers, and threats to EU cooperation in cyber strategies. Moreover, it will highlight areas of interest for further research and closes with prospects on the challenges at hand.

I. Basic Intergovernmentalist Assumptions

Neill Nugent states that "*Intergovernmentalism* refers to arrangements whereby nation states, in situations and conditions they can control, cooperate with one another on matters of common interest" (Neill Nugent, 2010, p. 428), which gives the leading role in international politics into the hands of states, respectively their governments. Here, one of the key-terms in intergovernmentalist approaches is sovereignty. It may be described as "[…] the legal capacity of national decision-makers to take decisions without being subject to external restraints" (Ibid.). Michelle Cini (2010) explains that intergovernmentalism itself is mostly influenced and moulded by "[…] realist or neo-realist analyses of inter-state bargaining" (p. 87). For intergovernmentalists, costs and benefits of European integration are in a permanent process of being weighted up against each other (Ibid., p. 88). Consequently "[t]he main aim in engaging in [the] qualitative cost-benefit analysis is to protect [EU Member State's] national interests" (Ibid., p. 89). Ben Rosamond (2000) stresses that the basic and underlying logic and family-wide trait for realism is that "[s]tates are seen as rational, unitary actors that derive their interests from an evaluation of their position in the system of states" (p. 131), with the main interest being that of survival through military strength in classical realism (Ibid.). As it is not mainly military strength through which this research wants to explain the strong reservation towards cooperation, classical realism would not embody a perfect choice for this research. Accordingly, Kenneth Waltz (2010) and his theory on structural realism must be mentioned as one of the ground laying authors for any recent intergovernmentalist approach in line with the introductory description of intergovernmentalism. A basic feature of Waltz' ideas is a system characterized by anarchy. Such an anarchic system, in which "[…] the state of nature is a state of war" (p. 102), dictates that "[…] the absence of government [which is anarchy], is associated with the occurrence of violence" (Ibid.). Waltz' rather systemic idea dictates that "[h]ow units stand in relation to one another […] is not a

property of the units. The arrangement of units is a property of the system (Ibid., p.80). The structure of that system is then constructed according to the "[…] arrangement of the system's parts and by the principle of that arrangement" (Ibid.). Ultimately, states all do share the same tasks, yet they are not similar "[…] in their abilities to perform them" (Waltz, 2010, p. 96). After all, it is the "[…] division of possible gains that may favour others more than itself", which worries a state (Ibid., p. 106). A cooperation-based use of assets would also create a situation in which a state is "[…] dependent on others through cooperative endeavors and exchange of goods and services" (Ibid.). Waltz further observes that in an anarchic world, there is "[…] no global agency to provide [global solutions]" (Ibid., p. 109). Additionally, Hanna Samir Kassab (2014) remarks that with the anarchical structure of the world in mind, "[…] cyber warfare is something to be expected […]", further adding that it may "[…] destroy a state's national security and autonomy and create a vulnerability that is so precarious, that its very survival, and that of its people, is at stake" (p. 62).

I.I Reasons for Choosing Two Intergovernmentalist Theories

Instinctively, one could argue that two opposing theories such as one intergovernmental, and one (neo-) neo functionalist could deliver a wider range of results, or be more beneficial for future research due to intensified controversy. However, both theories chosen for this research are picked exactly because they are similar in many of their characteristics. The benefit from choosing two partly complementary theories lies in the accentuation of their distinct differences. They are only roughly enumerated here, and will thus be thoroughly displayed in the following parts. Firstly, the most decisive difference is the formation of preferences of each EU Member State. While for Joseph M. Grieco these are formed as the result of the relative position inside the anarchic system, Andrew Moravscik accentuates a domestic formation of them. Knowing, how these initial preferences are formed, bears great value for any neo realist interpretation of cyber security related cooperation. Secondly, the idea of capabilities partly differs from the concept of bargaining-power, as the latter one accepts certain degrees of interdependence among states. As such, the interpretation of actions and execution of power differs, too. Thirdly, the explanation via voice opportunities diverges from that of liberal intergovernmentalist increases in credibility of commitments. The first aims for the accentuation of preservation of participation, while the latter aims for a decrease in defection. Revealing the differences in accentuation bears greater value for ongoing neo realist research on cyber security, than a broader and more adversarial choice of theories could ever achieve.

I.II Intergovernmentalism According to the Neorealist Assumptions of Joseph M. Grieco

The first EU integration theory depicted in this work is that of Joseph M. Grieco. Research conducted by Grieco (1999) exposed, why Germany and Japan developed such diverging concepts of dealing with their surrounding regions. One explanation given by Grieco is that through US influence, both operate differently. Accordingly, the potency of the USA to influence Japan via trade-matters was simply higher than in the German case (p. 118). Furthermore, Germany's security in central Europe was less dependent on the USA than that of Japan, which was surrounded by potential enemies (Ibid., p.122). Another factor possibly leading to Germany's interest in leadership through institutions could have been the fact that she was no completely hegemonic power like the US in the Americas. Yet, Japan did not use its clearly dominant position in East-Asia (Ibid., p. 115). Consequently, a country's position and goals inside the international system must be taken into consideration. Although survival remains the core interest of a state, it remains bound to its relative position. As such, bilateral and multilateral agreements always shape and define the behaviour of a nation state towards its surroundings. Grieco

(1988) further explains the importance of a relative position of power by contrasting neoliberal institutionalist and realist assumptions on this matter. While the latter do not only fear deception in cooperation and bargaining, but also that a partner achieves relatively greater gains, neoliberal institutionalists find that states are atomistic (p. 487). Hence, for neoliberal institutionalists, the "[…] utility function would be U = V" with U being the utility and V the payoff (Ibid., p. 497). Contrasting to that, Grieco (1988) proposes a realist utility function, which is U = V – k (W – V), with W being the partners payoff and k "[…] representing the state's coefficient of sensitivity to gaps in payoffs either to its advantage or disadvantage" (p. 500). His formula underlines the importance of the relative position of states in the international environment once again. With regards to Maastricht and the European Monetary Union (EMU), Grieco concludes that neo-realists could possibly argue that "[…] [Maastricht] represents an effort by the EC member states to enhance the Community's capabilities that is based on a rational assessment by each member of that strategy's costs and benefits" (1995, p.28). Examined from this perspective, actions initially seen as cooperative, could potentially be based on a national interest of individual gains. Grieco (1995) however underlines that for such an understanding, neo realists would at least need to reconsider their dismissive position against the perception of the importance of international institutions (pp. 28-29). Grieco (1995) enumerates several key problems that Maastricht caused for a neo realist understanding of the EU. These are the already mentioned underestimation of institutions, the need for a bipolar world order as well as for a balance in commitments and treaties, and above all state rationality being the consequence of anarchy (p. 32). He proposes to solve these issues with his theory on 'voice opportunities'. It allows for the explanation of smaller Member State's efforts to deepen cooperation by revealing that "[…] *the weaker but still influential partners will seek to ensure that the rules so constructed will provide sufficient opportunities for them to voice their concerns and interests and thereby prevent or at least ameliorate their domination by stronger partners*." (Grieco, 1995, p.34). While the important players seemingly coagulate their dominance, small- to medium players ensure their own influence. Yet, especially in the field of foreign politics and defence, the EU's capabilities to act are exposed as "[…] extremely limited […]" due to "[…] serious divisions […]" among Member States during crisis (Ibid., p. 22). Grieco's ideas are an invaluable asset to Waltz' basic work and show, how the applicability of intergovernmentalist logics may look like. His work is of such interest, as he consciously chose the EU when analysing state-behaviour. The tools and ideas he used in fields other than defence and security, may be most viable for the latter ones, too. Especially the interplay between relatively weaker and stronger states grants insights that are unique among neo-realist approaches. Combining the insights on Grieco, the following hypotheses can be drawn:

H1: If Grieco's assumptions are correct for the field of cyber security, EU Member States as the sole actors would aim for relative gains during cooperative efforts, and involved small- to medium players would follow the voice opportunity theory

This would be the case when …

a) Small- to medium EU Member States sacrifice sovereignty during a cyber-strategic cooperation for a guaranteed participation and voice during such cooperation.

b) EU Member States eschew cooperation once they relatively benefit less from it compared to the other involved party, or when the status quo itself is drastically imperilled. This is to be relativized if H1a is verified and actions accordingly allegeable by it.

Actions and decisions inside cyber security cooperation must reveal that EU Member States accentuate relative gains, which are the result of a cost-benefit-analysis. Important as well is the fact that decisions must be made at the national level without decisive influence coming from non-state actors of any sub-or supranational level. Firstly, for H1a the right application of Grieco's voice-opportunity theory demands that small-to medium important nation states behave in a way, which secures the right to partake in decisions in exchange for a lowered degree of sovereignty. Accordingly, these states must be part of a cyber-related commitment, which lowers their overall sovereignty for the sake of membership in a beneficial cooperation. Secondly, if H1b is true, the relative position of Germany, France and The UK will determine their strategic decisions in cyberspace and a behaviour according to Grieco's predictions will be visible. Additionally, the importance of states as the only relevant actors must be confirmed. The relativisation contained in H1b stems from important assumptions Joseph M. Grieco (1995) made with regards to possible minor misconceptions of neo realists, which are already listed above. Should H1a be verified, cooperation would not necessarily be prohibited in a situation, which allocates gains disproportionally at first sight. Disparities could be explained via additional indirect benefits for the presumably disadvantaged party. As such, the verification of H1b in its essence demands a detailed understanding of H1a.

I.III Intergovernmentalism Shaped as Liberal Intergovernmentalism According to Andrew Moravscik

Ben Rosamond (2000) describes Andrew Moravscik's ideas on liberal intergovernmentalism as the ultimate two-level game approach to European Integration (p. 136). What makes his theory so revolutionary, is the fact that it does not assume national preferences to be the consequence of a state's relative position in the system, but as the amalgamation of an interaction between state and society (Ibid., p. 136-137). Having created preferences this way on the national level, the second level of the game is the intergovernmental bargaining table of international politics (Ibid., p.137). Nugent (2010) explains that there are three crucial elements needed to understand liberal intergovernmentalism. Firstly, states are seen as rational actors, just as realism says. Secondly "[…] there is a liberal theory of national preference formation", which explains "[…] how state goals can be shaped by domestic pressures and interactions, which in turn are often conditioned by the constraints and opportunities that derive from economic interdependence" (p. 433). Lastly, all inter-state relations are intergovernmentalist in their nature, with their outcome being equal to a nation state's bargaining power (Ibid.). Cini's (2010) explanation of liberal intergovernmentalism adds that "[a] bargaining space […] is formed out of the amalgamation of national interests, with the final agreement determining the distribution of gains and losses" (p. 98). Consequently, more than just the state's interest in survival can be taken into consideration, when the topic of cyber security is contemplated, while additionally the accentuated importance of the state remains unharmed. Three important features of liberal intergovernmentalism were already established by Moravscik (1991), when the approach was still called intergovernmental institutionalism. The first requirement is that of interstate bargains, in which "[e]ach Government views the EC through the lens of its own policy preferences […]" (p. 25). These are, contrary to Grieco's intergovernmentalism, not simply given, but amalgamated "[…] by the preferences of of policymakers, technocrats, political parties, and interest groups" (Ibid., p. 26, Table 1). Secondly, in the absence of a European hegemon "[…] bargains struck in the EC reflect the relative power positions of the member states" (Ibid., p. 25), wherein the major states are the subject to threats of exclusion, while smaller ones are simply given side-payments (Ibid., p. 26). Lastly, to preserve their sovereignty, Member States of the EU prefer intergovernmental institutions instead of supranational bodies when making decisions (Ibid., pp. 26-27). Accordingly, the one last important

aspect has been introduced by Andrew Moravscik later during the revision of his liberal intergovernmentalist theory. While the two pillars of domestic preference formation, and intergovernmentalist bargaining do endure, he also stresses the importance of credibility. As such "[…] the pooling and delegation of sovereignty serve as mechanisms to increase the credibility of Member State commitments, particularly in areas where member governments (or their successors) would have a strong temptation to defect […]" (Moravscik, 1998, p. 9 as cited in Pollack, 2001, p. 232). The advantage of looking at the topic from both perspectives simultaneously is that it allows for the in- and exclusion of non-state actors, while the intergovernmental focus and logic remains unharmed in the process. Relating the EU-wide cyber security efforts of its Member States to the theory of liberal intergovernmentalism, the following hypotheses is proposed:

H2: If Andrew Moravscik's findings are correct for the field of cyber security, EU wide cyber strategic efforts would be the result of a two-level game, with national preferences being the result of domestic pressures and interactions, and an intergovernmentalist interaction based on each state's bargaining power.

This would be the case when …

a) Domestic groups and actors shape and determine the preferences of EU Member States.

b) Established and currently planned cyber-strategic efforts reflect the bargaining power of the involved EU Member States.

As with the hypothesis regarding Grieco's form of intergovernmentalism, certain elements are essential for liberal intergovernmentalism to be applicable to the field of cyber security, while the correct operationalization must be exerted as well. If H2 is true and liberal intergovernmentalism thus the right tool for explaining the EU wide efforts, all needed features will also be revealed in terms of cyber security. Yet, especially Moravscik's focus on economic questions must be regarded, when transferring the preconditions for liberal intergovernmentalism to cyber security. With regards to the hypotheses referring to liberal intergovernmentalism, the most important observations concern the national preference formation and the international bargaining. It must be clarified, whether (societal) key actors determine EU Member State preferences in cyber strategy. For the international bargaining, outcomes must reflect the partaking nation states' relative power. Furthermore, it must be stated that created institutions are by far not working against the power or sovereignty of nation states. Mark A. Pollack (2001) underlines that according to Moravscik, "[…] European integration actually strengthens national executives vis-á-vis their domestic constituencies, since COGs [Chiefs of Government] enjoy a privileged place at the Brussels bargaining table from which domestic interests are generally excluded" (p. 226). Contrary to Grieco's (1995) voice opportunity theory, liberal intergovernmentalism does not explain cooperation via safeguarding of participation, but with the elimination of threats embodied by defection and breach of contract.

I.IV Closing Remarks on the Chosen Theories

Just as it has been stated initially, the two theories show both, convergence and difference depending on the respective theoretical aspect. It is assumed at this point that a combination of both theories bears great value for further research. This thought will be carried into execution in section V. For now, having explained the two underlying theories and the established hypotheses, the next step demands an outlook on the national capabilities and goals of the chosen countries being France, the UK, and Germany. Developing these insights in a separate section allows for a precise accentuation of

similarities, as well as differences. The insights of section II will after that be combined with the prerequisites described in section I.

II. Cyber Strategic Capabilities and Goals of France, the UK, and Germany – Preface

This section provides an overview of the known capabilities and goals of France, the UK, and Germany in terms of cyber security. These EU Member States are, as stated above, deliberately chosen, as they embody three of the strongest among all of them, be it economic- or military-wise.

II.I France

The report of the French Network and Information Security Agency (ANSSI) (2011) mentions "[becoming] a cyber defence world power in cyber defence" as well was "[…] the protection of information related to [France's] sovereignty" as two of the main strategic objectives (p. 5). Among the chosen areas of action, the "[protection of] the information systems of the State and the operators of critical infrastructures", as well as the "[development of their] international collaboration" stand out as the two most characteristic ones (Ibid.). Interestingly is that France combines "[…] maintaining its strategic independence […]" with the participation in an "[…] inner circle of leading nations in the area of cyberdefence" (Ibid., p. 7). One could elaborate, whether being independent and part of a leading inner circle simultaneously is even possible. However, the idea behind independence seems to be a high degree of power-related capability. The ANSSI draws a connection between an information based society and economic competitiveness (2011, p. 11), while also underlining that "[…] foreign States or terrorist groups could attack the critical infrastructures of States that they consider as ideologically hostile" (Ibid.). Instead of preaching solo attempts however, the ANSSI remarks the importance of a "[…] network of allies […]", especially mentioning the European Union (Ibid.). Evaluating France's position in cyber capabilities, the ANSSI underlines that "France has world-class research teams in the areas of cryptology and formal methods. In other areas […] it is rapidly catching up with the most advanced nations" (2011, p. 16). The findings of the International Telecommunication Union (ITU) (2015) place France on sixth rank in the European region concerning cyber security. Especially the scores for legal aspects, capacity building and cooperation are comparably high, while the technical and organizational areas are still lacking in comparison (p. 15).

Europe	Legal	Technical	Organizational	Capacity Building	Cooperation	Index	Regional Rank
France*	1.0000	0.1667	0.5000	0.7500	0.6250	0.5882	6

[2]

At the moment, France has one officially recognized CIRT (Computer Incidence Response Team), the CERT-FR (Computer Emergency Response Team), and several other non-national CIRTs (Ibid., p. 197). In terms of capacity building, the ITU highlights the training center in the security of information systems (CFSSI), which "[…] is the main contact to ANSSI for agencies in charge of training" (Ibid., p. 198). Lastly, ANSSI has a number of official partnerships in form of (bilateral) agreements with Estonia, Germany, the Netherlands, the United Kingdom, the United States, and the European Union Agency for Network and Information Security (ENISA) (Ibid.). Its international affiliations are with FIRST, NATO, the EU, and the OSCE (Ibid., p. 199). A survey undergone by Booz Allen Hamilton (2011) compares the cyber power of chosen countries. Here too, France is placed on the sixth rank internationally (p. 4). Booz Allen Hamilton (2011) also rate France's score on technological infrastructure relatively low in

[2] ITU (2015): Global Cybersecurity Index & Cyberwellness Profiles, p. 15

comparison to other countries. While still being among the top seven nations, she remains on the last place and with a considerably lower score (Ibid., p.6).

Alexandra Jonas and Nicolai von Ondarza (2010) looked at the possibilities and hindrances in European defence integration. Von Ondarza (2010) observes for France, as well as for the UK that there are differences caused by the colonial past of the two. While the latter seeks to protect its oversea-territory, France mentions 1.5 million French citizens living in former colonies (p.45). Results are unique interests in distinctive global happenings and situations (Ibid.). The French will to shape and lead inside Europe is tangible (Ibid., p. 48).

The ENISA (2014a) furthermore summarized its findings in various fields such as the objectives, or the stakeholder involvement in cyber security strategies. While there are numerous resemblances between France, the UK, and Germany, there are also many drastically diverging findings. Due to a lack of space, they are not mentioned here, but pointed toward.

TABLE 1 Overall Cyber Power Rankings

Weighted sum of category scores (0-100 where 100=most favorable)

RANK	COUNTRY	SCORE
1	United Kingdom	76.8
2	United States	75.4
3	Australia	71.0
4	Germany	68.2
5	Canada	66.6
6	France	61.8
7	South Korea	59.7

[3]

II.II United Kingdom

The UK Cabinet Office (2011) focuses on aspects diverging from the French position, when tackling cyber strategies. For Great Britain, the first objective is defined as "[…] to tackle cyber crime and [being] one of the most secure places in the world to do business in cyberspace" (p. 8). The second and third main objectives are the protection of interests in cyberspace, as well as the support for open societies (Ibid.) The British National Cyber Security Programme has been funded with 650 Million £ over the course of four years (Ibid.). This programme is partly the reaction to the realization that "[t]he scale of [the UKs'] dependence means that [its] prosperity, [its] key infrastructure, [its] places of work and [its] homes can all be affected" (Ibid., p. 15). Knowing that the UK may not act entirely on its own, the UK Cabinet Office stresses the importance of "[…] strong international alliances based on shared values

[3] Booz Allen Hamilton (2011): Cyber Power Index. Methodology and Findings, p. 4

and common interests" (Ibid., p. 18). Underlining the importance of the Budapest Convention (tbdl.), the UK Cabinet Office also exerts that in appropriate cases, cyber-relevant sanctions are inside the possible range of actions (Ibid., p. 26).

According to the ITUs (2015) findings, the UK is regionally placed on the second rank. Outstanding are the scores for the organizational structure, as well as the capacity building. The latter possibly reflects the above mentioned heavy investments of recent years (p. 4).

Europe	Legal	Technical	Organizational	Capacity Building	Cooperation	Index	Regional Rank
Norway*	1.0000	0.6667	0.7500	0.8750	0.5000	0.7353	1
Estonia*	1.0000	0.6667	1.0000	0.5000	0.5000	0.7059	2
Germany*	1.0000	1.0000	0.6250	0.6250	0.5000	0.7059	2
United Kingdom	1.0000	0.6667	0.7500	0.7500	0.5000	0.7059	2

[4]

With regards to the CIRT efforts, the ITU (2015) asserts that by the end of 2014, a national CIRT was planned to be added to the already existing three governmental CIRTs (p. 490). Officially recognized and highlighted partnerships are established with the ITU, ENISA, TRUSTED, the European CERT Group, as well as the NATO (Ibid., p. 491). Even more impressive is the score of the United Kingdom given by Booz Allen Hamilton (2011, p. 4). During their conducted study, Great Britain is ranked as the internationally most advanced cyber power. Their technological infrastructure scored 37 more points than that of France (p. 6), while above all, the UK is even in a leading position compared to the United States.

II.III Germany

The German Federal Ministry of the Interior (BMI) declares a position somewhat between the French and British ones. It aims for an "[…] extension and moderate enlargement of the mandate of [ENISA] in view of the changed threa situation in ICT and the pooling of IT competences in EU institutions" (2011, p. 6), emphasizing cooperation to a certain degree. The BMI however also declares that "[Germany] will shape [its] external cyber policy in such a way that German interests and ideas concerning cyber security are coordinated and pursued in international organizations" (Ibid.). Important is that "The Cyber Security Strategy mainly focuses on civilian approaches and measures. They are complemented by measures taken by the Bundeswehr" (Ibid., p. 3), which exposes that a variety of actors are involved in terms of cyber security. Additionally, the involvement of the German *Länder* is another important aspect for the BMI (Ibid., p. 4). Generally, the German structure in terms of cyber security is relatively complicated and thus important for later discussions. With regards to the ITU (2015) ranking, Germany is placed on the second rank, just as the UK. Interestingly enough, it outperforms all other states with regards to the technical score. It has one recognized and legally mandated CERT (Ibid., p. 206). In addition to the international cooperation via EGC, TERENA, ENISA, FIRST, and APCERT, Germany has strong bilateral ties with the USA (Ibid., p. 207). Booz Allen Hamilton (2011) places Germany on the fourth rank. The fact that the UK is in a leading position especially in terms of the technological score may be the result of the calculational involvement of overall spending in the IT sector (see p. 14).

Von Ondarza (2010) stresses that Germany is still not allowed to take unilateral actions (p. 71). Thus, actions without UN-permission are highly problematic for Germany, whereas this is not the case for France and the UK (Ibid., p. 72). He further adds that the Franco-German cooperation has been

[4] ITU (2015): Global Cybersecurity Index & Cyberwellness Profiles, p. 14

struggling after 1994, as the white-books of both countries are no longer closely coordinated (Ibid., p.51).

Gerd Höfer (2008) analysed the possibilities and limitations of combined forces inside the EU. With regards to the German-French brigade, he says that it is a success based on the German-French cooperation. He does however also mentions problems, as for example the decision to create it was political and surprised the military, while it was also doubted military-wise (p. 118). Höfer inter alia mentions different Military Disciplinary Codes as more sources for possible problems. More severe are according to him the differences between "Auftragstaktik" and "Befehlstaktik", whereby the latter is stricter by showing both, the goal and the way to it. He does nevertheless says that such problems may be handled. However, whether deepened integration below the brigade is possible, remains to be seen in the future (p. 119).

III. EU-wide Cyber Security Efforts – An Overview

The most central document for the EU with regards to cyber security is the Cybersecurity Strategy of the European Union. Herein, the Commission set the basic principles and causes of action to be undergone. The underlying logic is that "[f]or cyberspace to remain open and free, the same norms, principles and values that the EU upholds offline, should also apply online" (2013, p. 2). Threats identified are "[…] including criminal, politically motivated, terrorist or state-sponsored attacks as well as natural disasters and unintentional mistakes" (Ibid., p. 3). Furthermore, while stressing the importance of cooperation, the Commission admits that it is "[…] predominantly the task of Member States to deal with security challenges in cyberspace […]" (Ibid., p. 4).

The strategy identifies five main goals to achieve (see Ibid., pp. 4-5):

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

Having these goals in mind, the Commission (2013) stresses that "[…] both public authorities and the private sector must develop capabilities and cooperate effectively" (p. 5). Whether the private sector indeed plays a role, will later be investigated especially with liberal intergovernmentalist assumptions in mind. With regards to the cyber defence dimension, the Commission asks Member States to "[…] concentrate on detection, response and recovery from sophisticated cyber threats" (Ibid., p. 11). Conspicuous is that these efforts concentrate on a rather defensive approach, and thus do not include measures clearly prescribed as retaliation. While again stressing the importance of the involvement of multiple actors, the Commission states that "[…] the EU will explore possibilities on how the EU and NATO can complement their efforts [...]" (Ibid.). Accordingly, the EU will also start a dialogue with nations that are seen as "[…] like-minded partners that share EU values", while in bilateral terms "[…] cooperation with the United States is particularly important […]" (Ibid., p. 15). With regards to the EU's main goals, Thomas Renard (2014) judged that "[w]hile this more integrated approach represents a step forward […] the EU is lagging well behind the US in this regard, not least because its member states are themselves lagging behind" (p. 11). Renard advises the EU to "[…] encourage its member states to invest more in their cyber security, with a view to turning Europe into a real cyber force" (Ibid.) He also notes that by stressing the cooperation with like-minded partners, countries "[…] such

as Russia or China, [are] thus implicitly dismissed" (Ibid., p. 12). Among the "[…] structured dialogues between the EU and its partners […]", the one with the USA, being the "[…] most developed in this regard […]", is executed "[…] mainly through the Working Group on Cyber Security and Cyber-crime […]" (Ibid., p. 15). Renard does state that the EU "[…] increasingly seeks cooperation and coordination with international actors, including strategic partners", however this does only happen with few of the international partners (Ibid.). Taking China, India, and Brazil out of the group of potential allies, relations with other partners "[…] [reflect] the marginal though nascence importance of [cyber-security] in these partnerships" (Ibid.). Despite all these difficulties however, Renard (2014) nevertheless underlines that "[…] the EU has emerged as a reliable international interlocutor on cyber issues" (p. 16).

Placed on the pillar embodied by the Cybersecurity Strategy of the European Union, is the EU Cyber Defence Policy Framework, which was adopted by the Council in 2014. One primary focus according to the Council "[…] [is] the development of cyber defence capabilities, made available by Member States for the purposes of the CSDP [Common Security and Defence Policy] as well as the protection of the European External Action Service (EEAS) communication and information networks relevant to CSDP" (2014, p. 3). Again, instead of tangible operations and setups, the framework demands minimum levels of cyber security, voluntary cooperation between CERTs, as well as exchanges (Ibid., p. 5). Furthermore, a "[…] unified chain of command […]" is only demanded for "[…] the conduct of CSDP operations and missions", while national authority over CERTs remains unharmed (Ibid., p. 6). What the Commission does not aim for is the creation of new international legal instruments, as it instead points towards the Budapest Convention (2013, p. 11).

The Budapest Convention, respectively The Convention on Cybercrime, to use the more appropriate term, is the main legal document for the EU with regards to measures in cyberspace. While being created already in 2001, it is still the worldwide uniquely binding legal framework for cyberspace. (Renard, 2014, p. 19). Renard further states that "Russia and China lead the charge [among the opponents]", while the position of states such as Brazil and India remains rather unclear (Ibid.). He however stresses that "[…] with around 50 signatories [the Budapest Convention] is not a global instrument" (Ibid., p. 24)

Neil Robinson (2014) explains that the development of "[…] military cyber-defence capabilities is a relatively 'greenfield' area for the EU" (p.1). According to Renard (2014), "[…] cyber security was identified as a key challenge in the review of the European Security Strategy (ESS) and, two years later, in the International Security Strategy (ISS)" (p. 10). What put the efforts a step forward was according to Robinson the revision of the Capability Development Plan (CDP), which was endorsed in 2011 (2014, p.1). Important institutions have been the EU Military Staff (EUMS) in cooperation with the European Defence Agency (EDA), as well as the Commission. All these initiatives are, according to Robinson, "[…] to a large extent coordinated with the comprehensive EU Cyber Security Strategy (EUCSS)" (Ibid.). Interestingly though, it was only since the CDP of 2010 that internal plans came into existence "[…] on what role the EDA should play in supporting the development of cyber-defence capabilities at member state level" (Ibid.). Robinson himself asserts that "[…] military force generation and readiness are a national (rather than EU) area of competence" (Ibid., p. 2), exposing that decision-making bears complicated multilateral organisation. Lastly, many countries are still unsure, whether the armed forces are the correct institution for the generation of cyber strategic capabilities (Ibid.). The NATO Cooperative Cyber Defence Centre of Excellence (CCDCoE) as a "[…] key provider of training and

education outputs […]" nevertheless represents "[…] an opportunity for quick wins in an area that is relatively uncontroversial and where there is significant demand from member states" (Ibid., p. 3).

Neelie Kroes, Vice-President of the European Commission responsible for the Digital Agenda stresses that "[…] if threats do not stop at national borders, nor does the responsibility to secure ourselves against them", promoting deepened cooperation (2013, p. 2). In this matter, Renard (2014) concludes that "[…] the EU has developed a flexible multi-layered approach, engaging with a variety of stakeholders at the multilateral, regional and bilateral levels" (p.11). Kroes however indirectly admits the rather national approach to security by recognizing that "[…] some [EU] countries are still not prepared enough: there are gaps in their capabilities". Filling these gaps is the responsibility of each Member State according to her (2013, p.3). Kroes (2013) however fervently defends the idea of cooperation among EU Member States and states that "[…] it shouldn't just be an exclusive club for the top performers" (p.3). She wishes to "[…] [leverage] existing work, like the European Public-Private Partnership for Resilience" (Ibid.), as well as increased cooperation efforts with "[…] partners like the US, Japan, OECD, OSCE, UN and ITU" (Ibid., p. 4). Despite that, the awareness for the importance of international cooperation was already in existence, when the European Security Strategy (ESS) came into existence in 2003. Already twelve years ago, it stated that "[…] no single country is able to tackle today's complex problems on its own" (Council of the European Union, 2003, p.1). It further elaborates on "[…] well functioning international institutions and a rule-based international order" as a main objective (Ibid., p. 9). With regards to the military capabilities, the ESS suggested "[…] pooled and shared assets […]" (Council of the European Union, 2003, p. 12) for an increase in overall strength. However, the Austrian Ministry of National Defence and Sport (BMLVS) remarks in its handbook on the CSDP that "[t]he ESS constitutes an important strategic choice, but it mostly tells [them] how to do things – it is much vaguer on *what* to do, it is incomplete in terms of objectives" (2010, p. 19). Accordingly, there is a gap between what the ESS aims for "and the practice of CSDP operations and capability development" (Ibid.). Ultimately, the BMLVS concludes that "[…] the question is what the EU, as the political expression of Europe and as a comprehensive foreign policy actor, wants to contribute as a global security provider […]" (Ibid.). Apparently, even a decade later, many pathways are not cleared and comprehensible.

The ENISA conducted research on the national cyber security strategies of several EU Member States. One of the most striking findings is that "[…] many countries do not agree on the outcomes or impacts of their NCSS [National Cyber Security Strategy] and on the ways to achieve them" (2014, p. iii). Important to know is that the ENISA bears no power to force a state to follow certain proceedings. Its task is to "[…] assist and support Member States in developing strong national cyber resilience capabilities […]" (Ibid., p. 5). The ENISA observes that "CERTs' presence, number and functions vary greatly between the Member States, according to a more or less centralised institutional system and assumptions about the role the new teams are supposed to play in implementing a secure cyberspace" (Ibid., p. 10), fortifying the assumption that efforts are still rather uncoordinated in that field. The ENISA is completely aware that "[…] in cyber security, there is no policy prescription that fits every situation". Despite this, ENISA nevertheless concludes that "[…] this inconsistency and fragmented approach belies a need for the application of broad framework through which NCSS can be evaluated […]" (2014, p. 36). Realizing this, a consistent framework could potentially enhance EU capabilities.

Von Ondarza (2010) observes that neither France, nor the UK, nor Germany mention trilateral cooperation amongst each other in their documents (p. 52). In general, von Ondarza (2010a) further explains that all three states do deliver military resources, yet they avoid being dependent on other

states (p. 132). He stresses this by mentioning the Airborne Warning and Control System (AWACS) and the diverging approach to this by the involved states (Ibid., p. 133). Jonas and von Ondarza (2010) further underline that recent initiatives stress horizontal cooperation with states being reluctant to give away state-centered sovereignty (p. 169). However, they also stress that especially the UK and France grew closer in their attempts to shape security. A stable balance of EU and NATO is sought, though the UK prefers a stronger NATO, while France favours a stronger EU (Ibid., p. 172).

Götz Neuneck (2013) observes that while the borderless entity of cyberspace would normally vouch for interstate-cooperation, "[…] there is a lack of a central international mechanism for discussing strategies – rather there is a plethora of potential forums all, with different focuses" (p.114). The findings for the EU do resemble the remark done by Neuneck, as there is also no real central power inside the EU managing cyber strategic efforts.

IV. Application of the Findings to the Proposed Hypotheses

After having introduced both, the various national approaches and strategies in terms of cyber security, as well as the EU treaties and agreements in question, this section interprets them and their relation to each other on the basis of the proposed hypotheses.

IV.I Relative VS. Absolute Gains

The initial question to answer will be, whether relative gains are pursued instead of absolute ones. Focusing on relative gains is a basic prerequisite for both hypotheses to be verified due to their intergovernmentalist nature.

The first key observation made by Alexander Klimburg and Heli Tirmaa-Klaar (2011) is that states such as Russia, and partly China, do seek to "[…] talk about cyber weapons […] and [to] treat these negotiations as essentially an arms-control issue […]" (p. 13). The authors furthermore note that "[m]ost Western nations have traditionally considered such a treaty to be hardly enforceable and open to abuse […]", while they promote the signature of the Budapest Convention "[…] to at least limit cyberattacks, including purported state-affiliated cyberespionage" (Ibid.). In accordance to Grieco (1988), it is possible to explain this via his contrasting juxtaposition of utility functions. In the liberal and atomistic case, the utility U of a disarmament in terms of cyber weapons (and thus capabilities) would equal the payoff V. Apparently, the equation U = V does not hold for cyber capabilities. Once the findings on the overall strength of Western countries in the dimension of cyberspace are applied to the circumstances, it becomes obvious why exactly that is the case. The Western countries are not atomistic in their view on the topic, as they know that they are in a leading position concerning cyber capabilities. Giving the inherently bound tools up for the sake of disarmament, would disadvantage them by comparison. What still exists in the equation U = V – k (W – V) is the utility of the payoff V. Yet, due to the potential abandonment of a nation's rank inside the hierarchy, a nation state such as Russia would comparably earn more payoff V, as its disused units and equipment are worth considerably less than that of for example Great Britain. This is further enhanced, when taking into consideration that according to Klimburg and Tirmaa-Klaar (2011), cyber power "[…] does not necessarily derive solely from the amount of trained hackers […] [but is] rather the sum total of resources or capabilities […]", which also include "[…] Critical Infrastructure Protection (CIP) […]" (p.15). Outstanding would be the loss for the United States, which "[…] probably [spend] more on cybersecurity than the rest of the world combined" (Ibid., p. 18). Clinging to the Budapest Convention and its only limiting effects is here the overall better choice for states with stronger capabilities in cyberspace. However, it must be mentioned that a large portion of CIP also include capabilities that

are "[…] not subject to direct government control and resides in non-state (i.e. business and civil-society) sector" (Ibid., p. 15). During this analysis they are added to the utility-function, yet they are not uniquely possessed by governments. On the contrary "[t]he private sector is responsible for virtually all of the software and hardware that is exploited in cyberattacks, maintains most of the network infrastructure where these attacks are conducted, and often owns the critical infrastructure that these attacks are directed against" (Ibid., p. 19). Accordingly, the cyber capability of a state should be extended by its potential power to cooperate effectively with its national cyber stakeholders. Even the smaller EU cyber powers and weaker Member States are among the signatories of the Budapest Convention. Their position in the system as closer allies of the Western European leading cyber powers is presumably the reason they cling to the treaty. However, the fact that the Russian, Chinese and US position in matters of the Budapest Convention directly affects the utility equation for EU Member States, shows that only with a careful analysis of global stances, EU cyber strategies do make sense.

Another fact that consolidates the importance of relative gains for the respective EU Member States is the reluctance to cooperate, when it comes to Critical Infrastructure Protection (CIP), and Critical Information Infrastructure Protection (CIIP). According to Klimburg and Tirmaa-Klaar (2011), advanced Member States, who already have strong CIP/CIIP capabilities "[…] only marginally support separate EU efforts in this field" (pp. 31-32). However, the authors also stress that due to CIP/CIIP being a "[…] multi-dimensional field that impacts not only legislation but also different layers of regulation and governance […]" the situation is more complex (Ibid., p. 32). Klimburg and Tirmaa-Klaar are optimistic in the sense that they do see that "[m]ost Member States are moving forward with major new EU initiatives in this area, such as supporting pan-European cyberexercises, adopting regulations for ISPs and enhancing information exchange" (Ibid.) Nevertheless, the combined insights on the national aims of France, the UK, and Germany and the fact that cooperation in CIP/CIIP is rather weak, hint toward the dominance of relative gains-cantered approaches. Additionally, the prospects mentioned by Klimburg and Tirmaa-Klaar (2011) all seem rather voluntary and non-binding.

Sascha Dietrich (2006) points toward a German-Italian position paper[5], wherein both countries proposed to use the EU's enhanced cooperation mechanism in matters of security and defence policy (p. 426). Elfriede Regelsberger (2001) inter alia adds that smaller EU states feared being marginalised and voted for higher minimum participation and the embedding in EU frame conditions (p. 156 (160) in Dietrich, 2006, p. 427). The fact that Regelsberger mentions the reservation of (presumably) weaker states towards the German-Italian proposition, reveals that their position paper contained advantages for stronger and more capable EU Member States.

Furthermore, actions concerning serious hardware-attacks[6] are not harmonized across the EU. Klimburg and Tirmaa-Klaar (2011) stress that nation states "[…] such as Russia, China, the US, but also France and the UK [sic!] have taken steps to protect against (or at least minimize) the threats […]", whereas "[…] these programs are not available to the EU or most EU Member States" (p. 36). The fact that there are indeed differences in power attribution is further underlined by Ryan David Kiggins (2014), who states that "[t]he US has the luxury of superlative technical skill among its cyber operators […] as evidenced by Stuxnet" (p. 166). Although granting the knowledge and capabilities to weaker EU Member States would enhance the overall structural defence of the EU, the UK and France reserve

[5] German Italian position paper 06.10.2000 Doc. CONFER 4783/00

[6] An attack based on physically manipulated chips, or other hardware. For a full description see Klimburg & Tirmaa-Klar (2011), p. 36

these to themselves despite their announced goal of cooperation. Having the dominance of the US in mind, withholding technology from European partners disadvantages the smaller states even more.

After explaining the main tasks and concerns of the European Defence Agency (EDA), Joylon Howorth (2013) remarks that "[…] it enjoys only a tiny budget […], a sign that governments remain uncertain about how far they can trust their own political instincts" (p. 13 in Sven Biscop & Richard G. Whitman, 2013). Sebastian, Duke of Kielmansegg (2005) underlines that until now, no Common Defence and Security Policy (CSDP) has been undergone by all EU Member States (p. 319 in Maike Kuhn, 2012, p. 143). The lack of an action undergone by all EU Member States simultaneously, illustrates the complexity of cooperation in the field of defence.

J.A. Lewis (2011), with regards to multilateral dialogue, concludes that "[t]he combination of a high degree of secrecy and weak research methodology complicate policymaking" (p. 55, as cited in Neuneck, 2013, p. 118).

Kai Biermann and Yashin Musharbash (2015) of Zeit Online analysed a document[7] regarding the XKeyscore software and a revealed deal between the US National Security Agency (NSA) and the German domestic intelligence agency (BfV). Although the article is highly appreciated, the detailed content of the document, as well as the capabilities of the program are of no interest here due to a lack of space. What needs to be underlined however is that instead of sharing the software and knowledge with fellow EU Member States, the deal concerning the software was struck between German and US intelligence. The prospect of relative gains apparently outmatched an overall increase in performance and capabilities of the EU as a whole.

Recapitulatory, it can be said that there are indeed many clues supporting the idea of relative gains being the predominant goal for nation states in cyber security efforts. The fact that stronger states do promote voluntary projects, try to evade binding commitments, and above all keep technological knowledge even from closest allies, fuels this impression. The first prerequisite for H1/H2 is thereby fulfilled.

IV.II H1a – The Voice Opportunity Theory

For H1a to be verified, small to medium EU Member States must sacrifice sovereignty during a cyber-strategic cooperation for a guaranteed participation and voice during such cooperation.

The first hints are again given by Klimburg and Tirmaa-Klaar (2011), who state that "[…] while some (mostly larger) Member States would proceed with cybersecurity issues at their own, a significant number of Member States are very much reliant on EU initiatives in this area […]" (p. 43). When separating the EU Member States in different categories in accordance to their size and advance in cyber strategic efforts, the authors furthermore do mention that for less advanced nation states "[…] their smaller size and limited resources compared to larger countries mean that cooperation (both internationally and nationally) is emphasized even more than among the larger states" (Ibid., p. 38). Intuitively, this would enhance Joseph M. Grieco's (1995) assumptions on the preservation of a voice and participation for a trade-off in sovereignty. Indeed, smaller EU Member States would benefit from cooperation in a more augmented way than for example France, or the UK. This is partly due to the facts highlighted with regards to the focus on relative gains in cyber security efforts.

[7] Source: http://www.zeit.de/digital/datenschutz/2015-08/xks-xkeystore-document

For another probable hint, the EU-US relations are taken into consideration as an important factor. Annegret Bendiek (2014) highlights that "U.S. cyberspace policy is driven increasingly by the military logic of deterrence […]. Europeans, […] treat the security aspects of cyberspace policy as a police matter, and their main goal is strengthening systemic resilience and resistance to attack and fraud" (p. 2). Both, the USA and the EU are on common ground with regards to their normative ideas, wishing the internet to be an open space for citizens, while leaving the internet itself as a legal subject inside national borders (Ibid., p.3). They also cling to a certain system of administrating cyber security issues. Both stress that the Internet Corporation for Assigned Names and Numbers (ICANN) should remain in charge, while "[a]uthoritarian states such as China, Russia, and Iran are pushing for an Internet regime that is more directly tied to the United Nations and in which national governments again acquire broad regulatory latitude" (Ibid., p. 4). Bendiek explains that this would give the power of locking out "[…] undesired users […]" from the internet to nation states (Ibid.). The ICANN however is not at all a perfect choice or tool. Bendiek (2014) explains that "[t]he role of national and supranational political bodies in these institutions is far from being authoritatively defined" (p.5). Why would EU Member States would want such a construct to be in charge? Firstly, without the legal permission to ban certain Internet Protocol (IP) addresses, authoritarian states find it harder to gain control over the use of the internet. This is in line with the promoted democratic values of both, the EU and the US. In addition to that, both may, due to their technological superiority, at least sometimes are enabled to track certain IP-addresses. They would thus also prevent a tool, which they themselves do not need, to come into existence. Secondly, being part of an organisation or institution, which is heavily biased by Western ideals, chances are that even in a situation of constraint, EU Member States' ideals are not so extensively violated. Although the US government seems to follow a more aggressive interpretation of cyber security, EU Member States do seem to favour it once the other possible scenario includes a boost in strength for states such as Russia or China. Furthermore, the ANSSI (2011) described Frances goals as fairly congruent with US ideals. To jump on the bandwagon, which promises at least increased chances for participation, is thus plausible. The result is the following: Small to medium EU Member States do consciously support ICANN dominance, because they know that the alternative would imply higher costs in the respective cost-benefit analysis. This is again an example of how international commitments may alter the strategic position and orientation of EU Member States.

Another important document is the Tallinn Manual written by the CCDCoE, which is "[…] designed to assist in adapting essential principles of international law to the conditions of the cyber age" (Bendiek, 2014, p.7). Ellen Nakashima (2012) & John Arquilla (2012) explain that the Tallinn Manual also seeks to explain, which "[…] conditions […] justify preemptive action against cyber attacks […]" (In Bendiek, 2014, p. 8). Here, the interpretation is done double-dealing, as the Stuxnet operation against Iran is sometimes regarded " as an act of preventive self-defense" (James A. Lewis, 2012 & Herbert Lin, 2012 as cited in Bendiek, 2014, p.8), while an attack on the New York Stock Exchange "[…] was ruled to have been serious enough to justify actions of self-defense" (Bendiek, 2014, p.8). In short, the US dominance based on the Tallinn Manual allows for a situation-related interpretation. Bandwagoning is thus again a possible choice for those who tolerate a limited US-dominance. Bendiek (2014) nevertheless rightly stresses that the Tallinn Manual inter alia "[…] provides a mutual point of reference for converging and diverging European and U.S. definitions of military attack, distinctions between civilian and military targets […]" (p. 7). It is thus a step forward in relations between the USA and Europe. Even more important are the implications for EU Member States. Even if the will for a mutual EU-wide cooperation would exist, the sheer dominance of the US may explain that single EU Member States prefer to work with them on bilateral terms.

With regards to the NATO Action Plan "[…] only a few member states have shown strong interest in implementing [it] or in participating in NATO cyber exercises, and neither Britain nor France belong to the active group" (Ibid., p. 9). Again, this shows not only that stronger EU Member States are willingly not participating in common efforts, but also that the weaker states are the ones, who would prefer such mechanics and setups. Furthermore, according to Rex Hughes (2011), "Russia wants to outlaw the use of cyber weapons in general" (in Bendiek, 2014, p. 11), while "[t]he United States does not" (Bendiek, 2014, p. 11). This is in part due to the fact that the United States would, as elaborated in the section above, give up more power comparatively (Ibid.). This should however not be understood as a new call for an arms race, as Bendiek (2014) stresses that "[…] since 2011, the EU and the United States have launched a number of joint initiatives to establish confidence and security building measures in relations with Russia and China" (p. 10). Yet, it is revealed that states such as Russia are eager to give up sovereignty in an exchange for security. Although being no EU Member State, it is to be assumed that without the protection of the EU and the close alliance to the US, many European smaller states would probably vote in favour of the Russian proposal.

There is however no unbreakable Western shield around the established institutions. Bendiek (2014) stresses that "some cracks seem to have emerged for the first time in the wall put up by Western states to prevent a reorganization of Internet governance", when the Edward Snowden incident occurred (p. 13). Giving up sovereignty in exchange for security did not work out as expected, thus the EU shows "[…] insistence on a more comprehensive inclusion of democratic countries such as Brazil and India" combined with a "[…] recent demand for greater inclusivity and transparency" (Neelie Kroes, 2013 in Bendiek, 2014, p. 13). Such an observation can only be made, when under the previous agreement the loss of sovereignty was tolerated by the small to medium Member States with the balance now being violated. Probably, in this case even France, the UK, and Germany have to be counted in as such because of the clear institution-wise dominance of the USA. The cyber strategies of EU Member States, and especially their cooperation among another is thus again influenced by shifting circumstances in global institutions. Important however is that according to Bendiek (2014) the multistakeholder model is not given up by the EU (p. 13). Accordingly "[…] the EU seeks to strengthen the Governmental Advisory Committee (GAC) of ICANN and with it the principle of intergovernmentalism" (Ibid., p. 14).

The observations made are in line with Joseph M. Grieco's (1995) assumptions on voice opportunities for small to medium nation states. Even nations regarded as the most powerful in terms of cyber security did seek to cooperate under US-dominance because of their institutional strength. However, once the advantages were offset by costs of espionage inside the alliance, EU Member States sought for other partners to slowly destabilize the dominant position of the US in exchange for renewed sovereignty.

IV. III H1b Eschewing Cooperation as a Result of an Unequal Distribution of Gains

For H1b to be verified, EU Member States must eschew cooperation once they relatively benefit less from it compared to the other involved party, or when the status quo itself is drastically imperilled.

The deliverables of the preceding parts do help to find a clear answer to this issue. It is already explained that relative gains are indeed the dominant kind of gains EU Member States are seeking for inside cyber security efforts. Especially the larger Member States did avoid giving more power to the central EU institutions. Apparently, they do fear that the status quo could be endangered once they commit themselves more than proportionally to EU-wide efforts. This is also partly due to the unique characteristics of cyberspace. Although servers are physically located in several countries, cyber defence is (mostly) non-physical and thus hardly comparable to military capabilities such as tanks. The

latter can be withdrawn, knowledge however sticks even after the break-up of a cooperation. Expertise and equipment needed to counter hardware-attacks is also withhold by the parties, who already have them in their arsenal. Thus, even physically removable assets are not given to weaker partners. Furthermore, servers physically located outside Europe are one of the reasons that deepened cooperation with the US are evaded to a certain degree. Their location "[…] gives quite far-reaching access rights to server providers", which results in the fact that "[…] U.S. authorities can easily gain access to the data of the Europeans who use [American] cloud-computing services […]" (Bendiek, 2014, p. 14). As this is no typical case of cyber-espionage, but poses a legal action, it can be assumed that it does not matter how high the actual cyber readiness and capabilities of the affected country and its citizens are. At this point, European cooperation may not be eschewed, as there is little choice but to replace global servers with European ones. The dominance of US IT-firms is just as problematic as the fact that "[…] most IT equipment is manufactured in Asia", which is why one of the only remaining solutions could be "[…] the creation of "national" technologies" (Ibid., p. 15). Such an approach is also suggested by W.K. Clark and P.L. Levin (2009, n.p. in Kassab, 2014, p. 69). Questionable however is, whether such technology would fall under the jurisdiction of the EU, or whether they are subjected to the respective law of a country, where the servers are located inside the EU. Truth is that China already executed a manoeuvre against the US. Richard A. Clarke and Robert K. Knake (2011) explain that the Chinese government pushed Microsoft to hand over its cruft and produced faked Cisco routers. These routers contained a weak spot to break through, while the Chinese systems used a different and modified software without this weakness (pp. 87-88). Relying on foreign hardware thus truly comes with a high risk. Recently, Spiegel Online received a confidential document regarding the stockpiling and centralisation of cyber capabilities. The strategy is part of the preparation for Germany's new *Weißbuch* (Matthias Gebauer, 2015). Instead of deepened cooperative European efforts, the main focus lies on the reconfiguration of national capabilities.

The Budapest Convention is what Stephen D. McDowell, Zoheb Nensey & Philip E. Steinberg may explain as a kind of limited cooperation. They conclude that while "[s]tates may not agree to all elements of a cooperative cybersecurity treaty, […] they might be able to agree on more narrow elements focused on specific criminal behaviour" (2014, p. 235). This is again reflected in the Budapest Convention. The authors do indeed say that "[g]iven the number of states and the diversity of political traditions there may be *few shared values* […]". They further denote that "[a]s an interstate institution, a cooperative security agreement would *enhance[s] the role of the state* […]". Interestingly though, they do perceive ICANN to be "[…] build upon the role of stakeholders rather than the preeminence of states" (Ibid., p. 235). This contradicts the observations made with regards to recent European actions, which strife for greater power for non US-dominated institutions. The sudden movement of EU Member States towards states such as Brazil, or India may not be explained, if the ICANN is perceived as a purely stakeholder-driven institution.

The unequal distribution of gains may also be explained via external effects. Following the ideas of Joseph Lepgold (1998), Christian Würdemann explains the external effect of conventional troops and atomic arsenals on third countries and that states can be excluded from such effects (In Würdemann, 2008, p. 71). For atomic weapons however, Todd Sandler & Keith Hartley (1995) do explain that in some cases especially atomic arsenals do create positive effects for third countries, which gain protection against a common aggressor (in Würdemann, 2008, p. 72). It can be assumed that the external effects for cyber security are even greater, as cyberspace knows no boundaries. Every cybercriminal or spy stopped by France, the UK, and Germany is a gain in security for all other EU

Member States. However, these strong states do profit much less from the weaker protection that smaller states contribute. Avoiding binding commitments and cooperation is thus logical for them.

Despite these insights, the EU is introducing financially well suited programs in the field of cyber security. Bendiek (2014) states that the between 2014 and 2020 about €80 billion are spend uniquely for the program "Horizon 2020", whereby €1,5 billion are used for security research purposes, and €400 million exclusively boost cyber security research (p. 19).

The combined observations from section IV.I and IV.III do indeed pose no threat to H1b. On the contrary, H1b can be verified by the gained insights. This however does not answer the question, whether state preferences are created domestically, or as the sole result of the position inside the international anarchical structure. This is where liberal intergovernmentalist assumptions come into play.

IV.IV H2a Domestic Preference Formation inside the EU – The German Case

Andrew Moravscik's liberal intergovernmentalism can partly be verified, when domestic groups and actors shape and determine the preferences of EU Member States. Revealing such circumstances is quite difficult, as it demands to penetrate the multileveled actions inside a country. Accordingly, out of the three cases, Germany has been picked as the single backing. The reasons for Germany in this case are the combination of firstly, the fact that it is population-wise the biggest EU country and therefore assumed to deliver enough complexity. Secondly, her historical accentuation of federal and multi-level structures, and lastly her position among the cyber-pioneering countries, do make her a reasonable choice.

A viable step towards clarification in this matter is to highlight the complex responsibilities even inside one single country. Arne Schönbohm (2012) describes the German "fragmented allocation of responsibilities" (p. 107) as the following:

"The Federal Ministry of Defence is responsible for the security of its own networks; the Federal Ministry of Food, Agriculture and Consumer Protection and the North Rhine-Westphalian Consumer Protection Centre jointly operate a website dedicated to the monitoring of phishing activity; and the Federal Ministry of the Interior (BMI) has responsibility for issues of cyber security at federal level. […] The Federal Criminal Police Office (BKA) maintains a Technical Service Centre (TeSIT) which deals with the Internet as a means or target of criminal activity. The Federal Office for the Protection of the Constitution (BfV) is also active in the field of cyber security within the scope of its counterintelligence brief" (Ibid., pp. 107-108)

Citing Schönbohm in a near entirety hopefully allows for an effect of wondrousness. The cyber strategic responsibilities inside Germany cannot be drawn in a more scaled down manner, yet they still demand a complex illustration. With both the *Länder* and the state itself being involved in cyber security, it is clear that there must be more than just one stakeholder in terms of cyber security issues. Sven Bernhard Gareis (2014) explains that even in the executive authority alone, several factors do come into play such as constellations of coalitions, or the personality of the German Federal Chancellor (p. 90). Furthermore, the distribution of power inside the parliament, lobbyists as well as other NGOs do play a role (Ibid.). In addition to that, the German Bundesrat as the representative body of the *Länder* does have great impact on EU politics, with its strength being way higher in EU matters than in common questions of foreign policy (Ibid., p.101). Accordingly, giving power to the central EU institutions also means that the executive authority also gives away power from the parliament to the *Länder.* With regards to new distributions of responsibility, Gareis further states that the ministers do insist on their sovereignty via the departmental principle (2014, p. 108).

With regards to non-state actors, Schönbohm (2012) mentions the Working Group on Security in Business (ASW), the German CERT-Verbund, Germany Safe Online (DsiN), the National Initiative for Data and Internet Security (NIFIS), as well as the German Digital Economy Association (eco) (pp. 80-83). The ASW has to be highlighted, as it is the "[…] German business world's central point of contact for security matters" (Ibid., p. 80) and thus a force to be reckoned with. Eco, representing firms "[…] which generate economic added value either within or using the Internet […] comprises around 500 domestic and international member firms, 7,500 contacts and 15,000 contact addresses" (Ibid, pp. 80-81). It is thus, too, a very important partner in terms of cyber security questions. This observations are also reflected in Klimburg and Tirmaa-Klaar (2011), as they criticise that "[…] many of the private sector initiatives in the Member States in this area (Public Private Partnerships and Information Exchanges) are often limited to 'national' companies and do not adequately reflect the cross-border nature of the private sector in Europe today" (p. 43). Though desired in a different manner, European interaction between different layers of industry, society and government seems rather limited. Adding to that, Bendiek (2014) underlines that "[…] intergovernmental relations in the transatlantic cyber partnership are robust and healthy, but its ties to civil society are feeble" (p. 25), which underlines the threat of "[…] governing practices [becoming] separated from the prerogatives of civil rights protection" (Ibid.). With regards to the dual-use control of exports, "[…] the German federal government expressly demanded that in the future, balanced consideration should be given to foreign and security policy issues as well as business interests" (2011, p.2 in Bendiek, 2014, p. 27). This again stresses the importance of economic actors inside and the complexity of the cyber security debate.

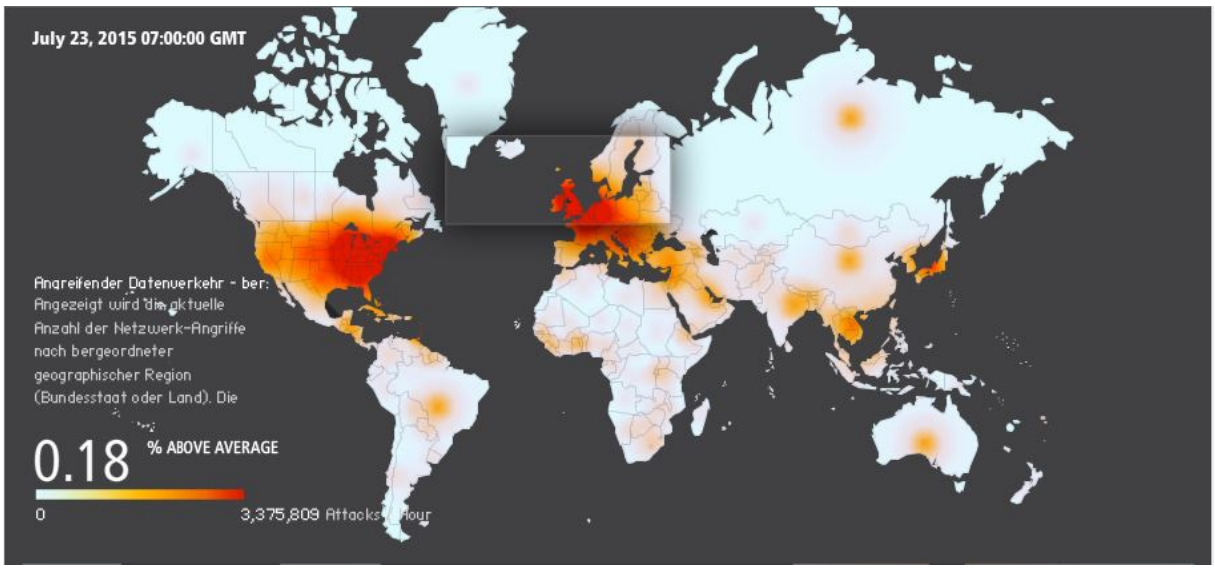
Although liberal intergovernmentalism does stress the importance of domestic actors with an intensified emphasis on economic actors, the public opinion should not be underestimated, especially in the German context. Heiko Biehl & Jörg Jacobs (2014) do stress that for the preservation of political power, actions against the dominant opinion (e.g. majority) in society are impossible (p. 274). Additionally, consensus is that security policy is withdrawn as much as possible from political calculatio (Ibid.). Facing the importance of the issue itself and its highly sensible interplay between society and the political body, the attitude of the German population must be counted in as an important factor. Trust in the German Bundeswehr peaked in 2000 with 65%, fell to 48% in 2002, yet rose to 59% in 2006 (Ibid., p. 273, Table 2). The trust values for the Bundeswehr are distinctively higher than those for the trade unions and the church, while the only institutions with a higher level of trust from society are the Police and the Federal Constitutional Court (Ibid.). Obviously, the Bundeswehr has been able to step up to the expectations of German citizens. Granted that the Bundeswehr and the Police are important actors in terms of cyber security, political decisions must be made with caution. Even more striking are those results dealing with acceptance towards certain Bundeswehr-orders. In 2012, 88% were accepting that the Bundeswehr should defend Germany itself, yet only 64% accepted the defence of a fellow NATO-state. Additionally, only 49% would accept the Bundeswehr being actively involved in peace-making battle operations mandated by the UN (Ibid.).

Of course, relative gains do also matter for Germany. Cooperation and more binding treaties could have been sought more intensively by Germany, would the case be any different. Yet, a strife for dominance, as mentioned by France, is nowhere to be found. Additionally, private and societal actors are the backbone for cyber resilience in Germany. Her position is by far not only constructed and enforced by the single thought of survival, but is an amalgamation of highly widespread capabilities and ambitions. H2a can be verified, which makes liberal intergovernmentalism indeed a beneficial tool when seeking for state preferences.

IV.V H2b Interstate Bargaining and Bargaining Power

H2b can be verified when established and currently planned cyber-strategic efforts reflect the bargaining power of the involved EU Member States.

At first glance, bargaining power does seem to be synonymous with overall capabilities. Yet, the bargaining power is, as stated above and in accordance to Cini (2010), a given window inside which the nation state might operate in bargaining. It is thus not based on a strife for survival backed by all its capabilities, but a strife for this window of demands that domestic groups have created, backed by exactly this window. Backed by this window, as the nation state can still juggle its position inside this small space. Yet, it is accepted that "[…] interstate bargains can lead on occasion to positive-sum outcomes" (S. Hix, 1999, p. 15 in Cini, 2010, p. 98). That is why "[…] governments will bargain hard to gain the upper hand" (Cini, 2010, p. 98). Factors for the interstate bargaining are the "[i]ntensity of national preferences, [a]lternative coalitions, [and] [a]vailable issue linkages" (Ibid., p. 97, Figure 6.1). Knowing for example that Germany amplifies cooperation more than France is a valuable with regards to their position towards bargaining. Hare (2009) tries to expose, which countries do have the highest interest in cyber security, and "which countries have the greatest imperative to work together due to their existing high level of inter-connectivity" (p. 11). For his sample, Hare used the bandwidth connectivity of the 21 greatest nation states, and revealed that Germany and the US are outstanding with their high number of connecting lines between them and other nations (Ibid., p. 98, Figure 1). This also implies that "[…] for most "non-central" nations [the security investment decision] is reduced immediately to a two-player game minimizing risk estimation" (Ibid., p. 99)



[8]

Shown in this graphic are the attacks on networks. Regions under heavy attacks are the US, Japan and the northwest of the EU. It is thus inevitable that these victims do seek to improve their network security. The difference between stronger and weaker European Member States is, as shown during this research, their capability to retaliate or counter such attacks. For the UK both, the attack rate, and the capability to counter them is presumably high. Yet, for states such as Italy the attack rate is high, while the capability to counter is presumably rather low. Logically, the latter will seek for cooperation that helps them. This has already been explained via the voice opportunity theory. However, smaller states efforts towards deepened integration may also be explained via domestic pressures. After all,

[8] Source: http://www.akamai.de/html/technology/dataviz1.html

fighting for participation in exchange for sovereignty can be the result of a position that has been formed domestically. It also bears the advantage that more than just survival and sovereignty are taken into consideration. This definitely needs further research in the future.

The fact that the larger and stronger EU Member States achieved a solution most viable to their national cyber strategies can be seen, when NATO and EU differences are analysed. One attempt to compare the roles and potentials of both NATO, and the EU is done by Piret Pernik (2014). Overall, he does say that cooperation between the two is both, plausible and desirable. There are however differences in setups and logics in terms of cyber security. For example, even though both accentuate the national responsibility, the EU lacks a central authority, while in NATO the NAC is in charge to fill in this position (p. 7). Furthermore, Pernik (2014) differentiates by saying that "NATO nations can request assistance through RRTs [Cyber Rapid Response Teams], while the EU […] functions as a forum for exchanging information and best practices" (p. 8). However, "[…] in contrast to the EU, NATO does not have a mandate to exercise authority or give guidance over civilian and private sector infrastructure" (Ibid.). This is a valuable insight because of slightly different responsibilities and powers. Would cyber attacks be retaliated just as attacks with armed forces, Article 42 VII TEU demands all Member States to help the attacked nation with all their capacities and power (EUV, p. 56). The NATO clauses, as stated above, are rather vague and open to interpretation, which makes it easier for nation states to drop out or in, depending on the attack. Should nation states be under attack, they "[…] are able to invoke the collective defence clause of the North Atlantic Treaty (Article 5) in case of a cyber attack with effects comparable to those of an armed attack" (Pernik, 2014, p. 6). While superficially demanding the same as the Treaty on European Union, NATO members may nevertheless evade involvement more easily, while even more importantly, the United States are possibly included in case of emergency. This does indeed changes the power balance drastically. Accordingly, it makes sense for stronger EU Member States to cling to rather weak European commitments, which they apparently did in the past. Pernik (2014) does stress that it is important for the future do determine, when the case of Article 5 may be invoked. Having a "[…] clear red line that obliges collective response when it is crossed […]" however, is "[…] undesirable for Nato […]" according to Pernik (2014, p. 10). Yet, he also denotes that "[t]he fact that the Alliance can launch a military response to respond to a cyber threat constitutes a major breakthrough in the development of NATO's approach to cyber security" (Ibid., p. 15). In terms of the EU however, the question remains, why strong EU Member States would vouch for common defence pooling, when "[…] of 2013, only 17 EU member states have [cyber security] strategies […]" (Ibid., p. 14). It does make sense for them to focus on partnerships with equally strong allies. Pernik (2014) indeed states that the EU has emerged as an important factor in terms of cyber security (p.15), yet the impression remains that there are many hindrances left. With the obligations and power still being centred in individual member states, it remains unclear, whether Pernik's (2014) hopes for deepened and joint cyber security efforts between NATO and EU may become reality.

An even more consentient view on deepened integration is represented by Hanna Ojanen (2006), who analysed in which ways neo-functionalists and intergovernmentalists perceived integration in the field of security in general. Specifically she analysed, in what ways the EU and NATO may exist in the future. Among other arguments, J. Howorth (2001) puts forward that "[…] a failure in ESDP [European Security and Defence Policy] would question the other political dimensions of the EU and also compromise the transatlantic relationship" (p. 773, in Hanna Ojanen, 2006, p. 66). This however does not mean an abandonment of the whole idea, but on the contrary that "[t]his binds the member countries to a common security and defence policy even though that policy field itself was not that binding as such" (Ibid.). While admitting that there are indeed efforts that aim for cooperation, there are clear hints

toward a stable reluctance to fully integrate cyber security efforts. Ultimately, Ojanen observes that "[t]he logic of EU integration means an eventual supranationalization of defence, while Nato logic keeps it traditionally intergovernmental" (2006, p. 69). She delivers two possible outcomes, being firstly "[…] an independent policy different from that of Nato, even as an alternative to it" (Ibid., pp. 71-72). The second option would be "[…] Nato […] supremacy over the EU in central questions of security and defence […]" (Ibid., p. 72). This paper suggests that the parallel existence of both organisations and the unclear distribution of power itself is benevolent for stronger EU Member States. Ojanen (2006) eagerly mentions many reasons for why security matters are not as immovable as they were and that integration is tangible. However, especially for the veto-powers France and the UK, both of them being nuclear powers, such an optimistic view is debatable. Their bargaining window is relatively small, when there is no proper compensation in new cooperation efforts for these two.

In any case, true for NATO is that among the issues inside the Alliance, Pernik (2014) mentions that top contributors to NATO's common military budget "[…] worry about who would have to pay for new capabilities" (p. 9). Additionally, "[…] more advanced member states, having heavily invested into national cyber capabilities, hesitate sharing these with others for financial and security reasons" (Ibid.). The seemingly deadlocked situation could be the result of the most powerful members being against intensified efforts and investments, reflecting their bargaining power in this matter.

It remains arguable, whether interstate bargaining is the overall better choice instead of a pure strife for relative gains. It does bear the advantage over the latter in admitting that there are indeed interdependences between nation states. This does add more complexity to the core questions of when nation states do decide to cooperate or not. However, as shown above, there are clues that indeed verify H2b.

V. Conclusion

Interestingly enough, all four hypotheses were verified throughout the research. How is that possible? Firstly, as elaborated in section I.III, it was expected right from the beginning that the chosen two theories would rather complement each other, instead of being polar opposites. Secondly, the nuances that do differentiate them do also leave a window for interpretation and make them even more comprehensible. It would thus be viable for the future not to try to pit the two theories against each other. They are adding such a diverse understanding to the discourse that they should indeed be fused, when talking about cyber security efforts inside the EU. It would be interesting to link the findings with the research conducted by Hare (2010), which aimed for making it possible to categorize nation states with regards to 'power' and 'socio-political cohesion'. The value lies not so much in the fact that he introduces these for the categorization itself, but in the assumed interaction of states. His observations could be mirrored against the voice opportunity theory, while also going beyond the idea of a pure strife for survival in the process of comparison is possible.

Having revealed that relative gains are the basic motivation for EU Member States, both, neo realism and liberal intergovernmentalism can be combined to a certain degree. While the voice opportunity theory helps us to understand, why the small to medium EU Member States are pledging for more cooperation whenever they can, it also possible to ascribe certain behaviour to the presumed strong nations, when they face institutional dominance of a third party, and thus certain restraints. The attribution "small to medium" should thus ultimately be seen as a relative and not an absolute term. Furthermore, the domestic preference formation may also be used for these states. Of course, this does collide with the basic realist assumption of survival as the prime goal. Yet, survival can also be the result of the domestic preference formation, which should be seen as an additive here. Liberal

intergovernmentalism could help to detect, in which ways survival emerges as the dominant motivation for a nation state to act. EU Member States did handle cooperative efforts with great caution, always trying to maintain the status quo. Whether this is due to their small bargaining windows, or simply their struggle for survival needs to undergo further research in the future.

What is clear is that intergovernmentalist approaches are still enabled to cope with the world, and are furthermore enabled to find and explain specific characteristics of cyber security efforts and cyber cooperation among EU Member States. That being said, the field of cyber security should not be regarded as a field, in which integration and convergence will either automatically, or in the near future be fully developed. On the contrary, the involved actors have to realize that caution and precaution still dominate the perception of cyber security. Thus, especially statesmen and European experts should further enhance the feasibility of bi- and multilateral agreements in this field for the coming years. With enough incentives, stronger and better prepared EU Member States could more likely share their knowledge. With enough compensation, weaker EU Member States could more easily agree to the dominance of a partner for the sake of increased overall-security. In the field of defence, units such as the German-French Brigade, or the German-Netherlands Corps were needed to create trust and a common understanding in many procedures. Europe should follow the same path in cyber security. This road may be rocky, yet there is no highway to convergence in sight.

VI. Limitations

The first and most serious limitation to the research conducted has been the fact that in many cases, data and information are classified. It is thus nearly impossible to directly compare EU Member States capabilities in numbers. Neither the exact amount of experts, soldiers, and scientists available to the respective cyber security programs, nor the location and size of operational bases is known. Through a variety of sources, this problem has been tackled as good as possible. Additionally, protocols on deals made on the bi- and multilateral level are also of course not completely available to the public. EU Member States' goals have thus been constructed as a result of their respective national strategies, combined with the insights of several researchers. Further ascription of goals would have been based on estimations, which has been consciously avoided.

Bibliography

Agence Nationale de la Sécurité des Sestémes d'Information (ANSSI) (2011): Information systems defence and security. France's strategy. Retrieved from: http://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf on 25.07.15

Arquilla, John (2013): Twenty Years of Cyberwar. Journal of Military Ethics, Vol. 12, No. 1, pp. 80-87

Austrian Ministry of National Defence and Sport (BMLVS) (2010: Handbook CSDP. The Common Security and Defence Policy of the European Union. Retrieved from: http://www.bundesheer.at/pdf_pool/publikationen/handbook_csdp-2nd-edition_web.pdf on 25.07.15

Bendiek, Annegret (2014): Tets of Partnership. Transatlantic Cooperation in Cyber Security, Internet Governance, and Data Protection, 2013-2014 Paper Series, No. 1, Washington DC: Transatlantic Academy

Arquilla, John (2012): Panetta's Wrong about a Cyber 'Pearl Harbour'. Foreign Policy, November 19, 2012

Cabinet of Germany (2011): Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Dr. Konstantin von Notz u.A., „Haltung der Bundesregierung bezühlich des Exports von ‚Dual-Use-Gütern' im Bereich der Technologie zur Störung von Telekommunikationsdiensten sowie Techniken zur Überwachung und Unterbrechung des Internetverkehrs durch deutsche Firmen", Berlin: Deutscher Bundestag, 17. Wahlperiode, Drucksache 17/8052, December 2, p. 2

Hughes, Rex (2010): A Treaty for Cyberspace, International Affairs 86, No. 2, pp. 523-41. Draft Convention on International Information Security, Jekaterinenburg, September 2011

Kroes, Neelie (2013): Building a Connected Continent, Speech 13/741, Brussels: European Commission, September 24, 2013

Lewis, James A. (2012): In Defense of Stuxnet, Military and Strategic Affairs, No. 3, pp. 65-76

Lin, Herbert (2012): Escalation Dynamics and Conflict Termination in Cyberspace, Strategic Studies Quarterly 6, No. 3, pp. 47-70

Nakashima, Ellen (2012): In Cyberwarfare. Rules of Engegement Still Hard to Define, The Washington Post, March 10, 2013

Biehl, Heiko; Jacobs, Jörg (2014): öffentliche Meinung und Sicherheitspolitik, in Böckenförde, Stephan (Ed.); Gareis, Sven Bernhard (Ed.) (2014): Deutsche Sicherheitspolitik. 2. Auflage, Opladen & Toronto: Verlag Barbara Budrich

Biermann, Kai; Musharbash, Yassin (2015): XKeyscore. A Dubious Deal with the NSA, Zeit Online. Retrieved from: http://www.zeit.de/digital/datenschutz/2015-08/xkeyscore-nsa-domestic-intelligence-agency on 03.09.15

Biscop, Sven (Ed.); Whitman, Richard G. (Ed.) (2013): The Routledge Handbook of European Security, Oxon & New York: Routledge

Howorth, Joylon (2013): European security institutions 1945-2010: the weaknesses and strengths of 'Brusselsization'

Booz Allen Hamilton (2011): Cyber Power Index. Findings and Methodology. Retrieved from: http://www.boozallen.com/media/file/Cyber_Power_Index_Findings_and_Methodology.pdf on 25.07.15

Cini, Michelle (Ed.); Borragán, Nieves Pérez-Solózarno (2010): European Union Politics. Third Edition, New York: Oxford University Press

Hix, S. (1999): The political system of the European Union, Basingstoke: Palgrave

Clarke, Richard A.; Knake, Robert K. (2010): Cyber War. The Next Threat to National Security and What to Do about It, New York: HarperCollins Publishers

Clarke, Richard A.; Knake, Robert K. (2011): World Wide War. Angriff aus dem Internet. Deutsche Ausgabe übersetzt von Heike Schlatterer und Stephan Gebauer, Hamburg: Hoffmann und Campe Verlag

Council of the European Union (2003): A Secure Europe in a Better World. European Security Strategy. Retrieved from: http://www.consilium.europa.eu/uedocs/cmsupload/78367.pdf on 25.07.15

Council of the European Union (2014): EU cyber Defence Policy Framework. Retrieved from: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/sede/dv/sede160315eucyberdefencepolicyframework_/sede160315eucyberdefencepolicyframework_en.pdf on 25.07.15

Diedrichs, Udo (2012): Die Gemeinsame Sicherheits- und Verteidigungspolitik der EU, Wien: Facultas Verlags- und Buchhandels AG

Dietrich, Sascha (2006): Europäische Sicherheits und Verteidigungspolitik (ESVP). Die Entwicklung der rechtlichen und institutionellen Strukturen der sicherheits- und verteidigungspolitischen Zusammenarbeit im Europäischen Integrationsprozess von den Brüsseler Verträgen bis zum Vertrag über eine Verfassung für Europa, Baden-Baden: Nomos Verlagsgesellschaft

Regelsberger, Elfriede (2001): Die Gemeinsame Außen- und Sicherheitspolitik nach „Nizza“ – begrenzter Reformeifer und außervertragliche Dynamik, in Integration 24

ENISA (2014): An evaluation Framework for National Cyber Security Strategies. Retrieved from: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/an-evaluation-framework-for-cyber-security-strategies-1 on 25.07.15

ENISA (2014a): Annex A: Mapping of cybersecurity strategies (September 2014). Retrieved from: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/an-evaluation-framework-for-cyber-security-strategies-1/annex-a-mapping-of-countries on 25.07.15

European Commission (2013): Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Retrieved from: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf on 25.07.15

Gareis, Sven Bernhard (2014): Die Organisation deutscher Sicherheitspolitik – Akteure, Kompetenzen, Verfahren und Perspektiven, in Böckenförde, Stephan (Ed.); Gareis, Sven Bernhard (Ed.) (2014): Deutsche Sicherheitspolitik. 2. Auflage, Opladen & Toronto: Verlag Barbara Budrich

Gaycken, Sandro (2012): Cyberwar. Das Wettrüsten hat längst begonnen. Vom digitalen Angriff zum realen Ausnahmezustand, München: Wilhelm Goldmann Verlag

Gebauer, Matthias (2015): Geheime Bundeswehr-Strategie: Von der Leyen rüstet an der Cyberfront auf, Spiegel Online. Retrieved from: http://www.spiegel.de/politik/deutschland/bundeswehr-ursula-von-der-leyen-ruestet-an-der-cyber-front-auf-a-1042985.html on 03.9.15

German Ministry of the Interior (BMI) (2011): Cyber Security Strategy for Germany. Retrieved from: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/Germancybersecuritystrategy20111.pdf on 25.07.15

Grieco, Joseph M. (1988): Anarchy and the Limits of Cooperation: A Realist Critique of the Newest Liberal Institutionalism. International Organization, Volume 42, Issue 3, pp. 485-507

Grieco, Joseph M. (1995): The Maastricht Treaty, Economic and Monetary Union and the neo-realist research programme. Review of International Studies, 21, pp. 21-40

Grieco, Joseph M. (1999): Realism and Regionalism. American Power and German and Japanese Institutional Strategies During and After the Cold War, New York: Columbia University Press

Hare, Forrest; Czosseck, C. (Ed.); Podins, K. (Ed.) (2010): The Cyber Threat to National Security: Why Can't We Agree? Conference on Cyber Conflict. Proceedings 2010, Tallinn: CCD COE Publications

Hare, Forrest (2009): Borders in Cyberspace: Can Sovereignty Adapt to the Challenges of Cyber Security? in Czosseck, Christian (Ed.); Geers, Kenneth (Ed.) (2009): The Virtual Battlefield: Perspectives on Cyber Warfare, Amsterdam: IOS Press

Höfer, Gerd (2008): Europäische Armee. Vision oder Utopie?, Hamburg: merus Verlag

Hönicke, Fabian (2014): Possibilities and Limits in allocating Cyberwar along the dimensions of Realism and Liberalism

International Telecommunication Union (ITU) (2015): Global Cybersecurity Index & Cyberwellness Profiles. Retrieved from: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf on 25.07.15

Jonas, Alexandra; von Ondarza, Nicolai (2010): Schlussfolgerungen und Empfehlungen, in Jonas, Alexandra; von Ondarza, Nicolai (2010): Chancen und Hindernisse für die europäische Streitkräfteintegration. Grundlegende Aspekte deutscher, französischer und britischer Sicherheitspolitik im Vergleich, Wiesbaden: VS Verlag für Sozialwissenschaften

Kassab, Hanna Samir (2014) In Search of Cyber Stability: International Relations, Mutually Assured Destruction and the Age of Cyber Warfare, in Kremer, Jan-Frederik (Ed.); Müller, Benedikt (Ed.) (2014): Cyberspace and International Relations. Theory, Prospects and Challenges, Berlin & Heidelberg: Springer-Verlag

Clark, W.K.; Levin, P.L. (2009): Securing the information highway. Foreign affairs. Retreived by the authors from http://www.foreignaffairs.com/articles/65499/wesley-k-clark-and-peter-l-levin/securing-the-information-highway on 12.09.2012. Article is also available under: https://www.foreignaffairs.com/articles/united-states/2009-11-01/securing-information-highway

Kiggins, Ryan David (2014): US Leadership in Cyberspace: Transnational Cyber Security and Global Governance in Kremer, Jan-Frederik (Ed.); Müller, Benedikt (Ed.) (2014): Cyberspace and International Relations. Theory, Prospects and Challenges, Berlin & Heidelberg: Springer-Verlag

Klimburg, Alexander; Tirmaa-Klaar, Heli (2011): Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action within the EU. Retrieved from: http://www.europarl.europa.eu/RegData/etudes/etudes/join/2011/433828/EXPO-SEDE_ET%282011%29433828_EN.pdf on 06.08.15

Krasner, Stephen D. (1991): Global Communications and National Power: Life on the Pareto Frontier. World Politics, Vol. 43, No. 3, pp. 336-366

Kroes, Neelie (2013): Towards a coherent international cyberspace policy for the EU. Retrieved from: http://europa.eu/rapid/press-release_SPEECH-13-82_en.htm on 25.07.15

Kuhn, Maike (2012): Die Europäische Sicherheits- und Verteidigungspolitik im Mehrebenensystem © by Max-Planck Gesellschaft zur Förderung der Wissenschaften, Heidelberg: Springer

Duke of Kielmansegg, Sebastian (2005): Die Verteidigungspolitik der Europäischen Union, Stuttgart: Richard Boorberg Verlag GmbH & Co KG

McDowell, Stephen D., Nensey, Zoheb; Steinberg, Philip E. (2014): Cooperative International Approacges to Network Security: Understanding and Assessing OECD and ITU, in Kremer, Jan-Frederik (Ed.); Müller, Benedikt (Ed.) (2014): Cyberspace and International Relations. Theory, Prospects and Challenges, Berlin & Heidelberg: Springer-Verlag

Moravscik, Andrew (1991): Negotiating the Single European Act: National Interests and Conventional Statecraft in the European Community. International organization, Vol. 45, No.1, pp. 19-56

Neuneck, Götz (2013): Chapter 2: Assessment of international and regional organizations and activities, in The Cyber Index. International Security Trends and Realities, New York & Geneva: United Nations

Lewis, J.A. (2011): Confidence-building and international agreement in cybersecurity, Disarmament Forum, No. 4., p. 51

Nugent, Neill (2010): The Government and Politics of the European Union. 7th Edition, New York: Palgrave Macmillan

Ojanen, Hanna (2006): The EU and NATO: Two Competing Models for a Common Defence Policy, JCMS, Vol. 44, No. 1, pp. 57-76

Howorth, J. (2001): European Defence and the Changing Politics of the European Union: Hanging Together or Hanging Separately? Journal of Common Market Studies, Vol. 39. No. 4, pp. 765-789

Von Ondarza, Nicolai (2010): Allgemeine Leitlinien in der Sicherheits- und Verteidigungspolitik, in Jonas, Alexandra; von Ondarza, Nicolai (2010): Chancen und Hindernisse für die europäische Streitkräfteintegration. Grundlegende Aspekte deutscher, französischer und britischer Sicherheitspolitik im Vergleich, Wiesbaden: VS Verlag für Sozialwissenschaften

Von Ondarza, Nicolai (2010a): Verfechter eines wirksamen Multilateralismus? Sicherheits- und Verteidigungspolitik auf der internationalen Ebene, in Jonas, Alexandra; von Ondarza, Nicolai (2010): Chancen und Hindernisse für die europäische Streitkräfteintegration. Grundlegende Aspekte deutscher, französischer und britischer Sicherheitspolitik im Vergleich, Wiesbaden: VS Verlag für Sozialwissenschaften

Pernik, Piret (2014): Improving Cyber Security: NATO and the EU. Retrieved from: http://www.icds.ee/fileadmin/media/icds.ee/reports/Piret_Pernik_-_Improving_Cyber_Security.pdf on 06.08.15

Pollack, Mark A. (2001): International Relations Theory and European Integration. Journal of Common Market Studies, Vol. 39, No. 2, pp. 221-44

Moravscik, Andrew (1998): The Choice for Europe: Social Purpose and State Power from Messina to Maastricht, Ithaca: Cornell University Press

Renard, Thomas (2014): The rise of cyber-diplomacy: The EU, its strategic partners and cyber-security. ESPO working paper 7, Madrid: FRIDE

Robinson, Neil (2014): EU cyber-defence: a work in progress. European Union Institute for Security Studies. Retrieved from: http://www.iss.europa.eu/uploads/media/Brief_10_Cyber_defence.pdf on 25.07.15

Rosamond, Ben (2000): Theories of European Integration, New York: Palgrave Macmillan

Schönbohm, Arne (2012): Germany's Security. Cyber Crime and Cyber War, Münster: Edition Octopus in Verlagshaus Monsenstein und Vannerdat OHG

UK Cabinet Office (2011): The UK Cyber Security Strategy. Protecting and promoting the UK in a digital world. Retrieved from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf on 25.07.15

Waltz, Kenneth N. (2010): Theory of International Politics, Long Grove: Waveland Press, Inc.

Würdemann, Christian (2008): Europäische Integration und äußere Sicherheit. Kompetenzverteilung zwischen Zentralisierung und Dezentralisierung, Berlin: Verlag Dr. Köster

Lepgold, Joseph (1998): NATO's Post-Cold War Collective Action Problem, in: International Security, Vol. 23, pp. 78-106

Sandler, Todd; Hartley, Keith (1995): The economics of defense, Cambridge: Cambridge University Press

Ziercke, Jörg (2013): Cybercrime – Bedrohung, Intervention, Abwehr. BKA-Herbsttagung. Kriminalistik 2.0 – effektive Strafverfolgung im Zeitalter des Internet aus der Sicht des BKA. Retrieved from: http://www.bka.de/nn_243818/DE/Publikationen/Herbsttagungen/2013/Redebeitraege/herbsttagung2013Redebeitraege__node.html?__nnn=true on 25.07.15