THE EUROPEAN UNION AS NORM ENTREPRENEUR

Promoting Global Cyber Diplomacy

Carl Tobias Reichert

The Hague, Netherlands

May 2017

Master Thesis

Adv. MSc. International Relations and Diplomacy

Universiteit Leiden

Carl Tobias Reichert

S1762486

22.05.2017

Presented to the Faculty of Global Governance and Global Affairs of the University of Leiden in partial fulfilment of the requirements for the degree of Advanced Master of Science in International Relations and Diplomacy.

First Reader - Prof. Madeleine Hosli

Second Reader - Dr. Peter van Ham

ABSTRACT

Cyber security is the policy issue of the hour. The threat and damage of cyberattacks, both for criminal and political gains, has dramatically increased in the past years. Yet, the internet is one of few transnational domains where actors disagree how to best regulate and govern the complex political, economic and social issues that arise. The European Union can play an important role in setting norms for appropriate behavior in cyber space. The concept of European normative power describes the uniqueness of European power, which is fundamentally anchored in multilateralism and the promotion of values. This thesis explains how the European Union attempts to promote its vision of the internet, spelled out in the European Cyber Security Strategy, with the tool of cyber diplomacy towards other relevant actors on a global level. It is argued that the European Union attempts to present itself as a norm entrepreneur. Examining the cyber security strategies and partnerships with the USA, India and Russia, the research finds that whilst the EU has managed to become an important interlocutor on cyber issues, it has not yet successfully acted as a norm entrepreneur.

Keywords : EU, cyber norms, cyber security, cyber diplomacy, norm entrepreneur

ACKNOWLEDGEMENTS

First and foremost, I would like to thank Professor Madeleine Hosli not just for guidance and encouragement in writing this thesis but for making MIRD what it is today. Without her, this program would not exist and I am eternally thankful for having been part of it. Special shout out also to Ragnhild Drange, for all the gossip and coffees, and always lending an open ear in times of distress.

Further, I want to thank everyone in the program for making the last two years so special and enriching, academically but also on a personal level. We were together when the world as we know it became increasingly somber and without the humor and wits of my classmates, it would have been even harder to grasp. Special thanks go out to Alex and Nick, who made both thesis writing and life in general so much brighter. Laughter is the best medicine against anything, and you provided me with plenty.

Lastly, all my thanks go out to my family and Kathi. Without the support of both my parents I would not have been able to sit here. Without the encouragement, endless support and understanding as well as proofreading of Kathi I would not have written such a thesis. Thank you!

Table of Contents

1. Introduction

Cyber security is the policy issue of the hour. Events such as the Stuxnet attack on an Iranian nuclear enrichment facility in 2010, the cyberattacks on Estonia in 2007 and the alleged Russian hacking during the U.S. elections 2016 have brought the issue to the top of the agenda. Recently, the ransomware 'Wanna cry' shook the whole world, with the British healthcare system NHS in particular targeted. This again demonstrated the need to resilient cyber security systems, as such an attack can have direct implications on life and death of citizens. The European Institutions have also been a victim of cyber-attacks, when in 2011 a breach of the emission trading scheme has caused a loss of around 30€ million worth of carbon emission allowances (House of Lords 2011). However, despite a shared sense of urgency to organize, protect and keep the cyberspace, several challenges arise when researching on this topic. Whilst intuitively people understand the meaning of cyber security, there is no commonly shared and accepted definition of what cyber security actually entails. Yet, a shared understanding is of paramount importance, as different definitions will lead to different focuses and policy measures. The way in which issues are framed influences threat perception, as well as what measures are needed and justified.

The transnational nature of cyber activities also indicates that national responses alone are not sufficient. Indeed, the European Union (EU) has brought forward a courageous and far-reaching proposal for an EU directive to be incorporated into EU member state legislation. It is one of the first attempts to legislate cyber security in a multilateral framework. Furthermore, an EU cyber strategy has been published in 2013, which spells out priorities for governments and the EU on how to deal with the phenomenon. Recently, another term has arisen which aims to capture the efforts of the EU: Cyber Diplomacy. Cyber diplomacy is a buzzword, which mainly describes the attempt of the EU to establish partnerships with key actors, such as the US, India, China and Russia, and multilateral organizations in order to work towards a form of international internet governance. The term has been coined through European council conclusions in 2015, in which the heads of state and government called for greater European cyber diplomacy and internet governance. It has since then also been picked up by the European External Action Service (EEAS) in order to incorporate this notion into EU foreign policy efforts.

The idea of internet governance is born out of the fact that the applicability of International Law in cyber space, without a doubt an inter- and transnational phenomenon, is contested. By seeking these partnerships and attempting to formulate shared norms for cyber space the EU is seeking to promote shared values which at a later stage might even lead to an international legal cyber framework. However, such a notion is still far from realistic.

The EU is considered by some scholars and policy makers as a 'civilian power' or 'normative power'. This may also be translated into the cyberspace and indeed, the proposed directive posits that 'Governments have several tasks: to safeguard access and openness, to respect and protect fundamental rights online and to maintain the reliability and interoperability of the Internet'. As spelled out in the cyber security strategy, the values and norms upheld by the EU should apply both offline and online. The concept of European normative power is closely linked to the constructivist theory of norm entrepreneurship. This term has been coined by Finnemore and Sikkink (1998), and describes an actor which pushes certain norms via the 'norm life cycle' until they become widely shared values and norms. I argue in this thesis that the EU is acting as a norm entrepreneur in shaping and regulating a global notion of cyber space governance. By seeking partnerships with key actors, it aims to shape internet governance. However, the success of these partnerships is highly contested. The research question of this thesis is therefore: *How is the European Union as normative power promoting global norms of cyber security?* More specifically, the thesis will scrutinize to what extend the tool of cyber diplomacy and key partnerships contribute to promoting these norms. More generally, the thesis analyzes whether such partnerships contribute to European normative power as the EU emerges as norm entrepreneur.

Much of the research on European cyber power closely scrutinizes the internal dimension of the EU, as much of these capabilities lie in the hands of the member states (MS). However, the transnational nature of cyber security forces the EU to also cooperate outside of the European continent. Therefore, the topic assesses whether the EU is indeed a successful diplomatic actor and is capable of being a 'great power' among China, the US and Russia. By contributing to this question, the thesis will address real world challenges that the EU faces. As is evident from above, several notions and dimensions need clear definition in order to examine the relationship, concepts, variables and indicators. Cyber security, cyber diplomacy and normative power need to be scrutinized and defined closely. The proposed EU directive

and key partnerships then provide real world evidence to test whether its governance indeed contributes to the EU as a civilian power. By including the constructivist theory of the norm life cycle and the EU as a normative power, this thesis addresses a research gap. Until now, research is focused on the internal dimension or indeed the efforts of single member states in cyber security. By addressing key partnerships, this thesis may contribute to the debate of the EU as a normative power in the world.

The thesis first explores the notion of European normative power and links it to norms research in international relations. These sections lay out how norms are furthered and what role a norm entrepreneur takes on the global stages as well as the instruments used. As the section on normative power demonstrates, specific non-coercive instruments are used in order to push for global norm building. In a second step, the thesis will describe the internal and external dichotomy of European cyber norm building and demonstrates that these dimensions are highly interlinked. Special attention is paid to the term cyber diplomacy, which is the tool to act as a norm entrepreneur. The methodological section lays out the comparative case studies and research design.

The case studies, in form of a comparative case study, focus on three actors, the US, India and Russia. These represent various degrees of partnerships and first map the current cyber relations, the understanding of cyber norms of these actors and finally address how and whether the EU indeed acts as a norm entrepreneur in furthering the EU's notion of cyber norms. The discussion section then recalls the findings and links it back to the theoretical section.

2. Theoretical Framework

2.1. The EU as Normative Power

The debate on the European Union (EU) as a foreign policy actor in its own right, has been subject to discussion since the Cold War. Interpretations vary greatly of the EU as an actor, from an irrelevant one in global relations (Kagan 2008) to the EU as one of the three main empires of the twenty-first century (Khanna 2008). The wide array of interpretation largely stems from two conditions exclusive to the EU (Gerrits 2009): Firstly, the EU as an

institution *sui generis*, fundamentally novel and unique in its design, especially in regards to its role as an international actor. Secondly, the *distinct* form and influence of European power globally; an economic power house with little military might. This is usually put in stark contrast to notions of power of other actors such as the US and China, which traditionally also rely on forms of hard power.

This chapter will first outline the roots of the debate on the EU as a distinctive soft power wielder, juxtaposing this notion to the discussion on European identity and legitimacy. From there, this chapter scrutinizes two concepts of the debate which bear particular relevance for this thesis; the EU as normative power and as promoter of cosmopolitan law. Before addressing this concept in more detail in the next chapter, this chapter will highlight some of the criticisms that the debate on the EU as normative power has sparked.

The different notions of the distinct form of European power can, to a large extend, be traced back to an article by François Duchêne in 1972, where he coined the term of the EU as a civilian, explicitly non-military, power (Duchêne 1972). This should be seen in the context of the Cold War, in which the – then European Community (EC) – found itself between the two great powers USSR and USA. The emergence of great non-military powers such as Japan and Germany, as well as the fading military might of US military dominance in Southeast Asia and a détente in East-West relations, inspired Duchêne to conceptualize a form of power going beyond sheer conventional military might (Gerrits 2009). The relevance as a foreign policy actor thus stems not so much from coercive measures (economic power is excluded from that list), but rather 'the attractiveness of its example' (Gerrits 2009, 2). By reflecting diverse practices, norms and values such as democracy, human rights and multilateralism, it developed a power in its own right. Much has been written and researched since Duchêne's article, with different authors finding different names for this kind of power by attraction from 'post-modern power' (Telò 2007) 'ethical' (Aggestam 2008) to 'soft' (Nye 2004, 2002) and 'normative' (Manners 2002). These concepts commonly stress that the values and objectives of the EU are promoted differently to those of the superpowers. Smith identifies these as a strong support in economic stability, which is considered as important for political stability by the EU (K. E. Smith 2000). Respect for human rights is to be promoted through quiet diplomacy and long-term interdependence, regional cooperation and the willingness to develop supranational structures to address critical issues of international management (Maull 1990).

Military power is only kept as residual instrument in order to safeguard other means of international interaction. According to Gerrits however, it was the 'radical unilateralism' by George W. Bush in 2003 which was most supportive in creating a European (self-) perception as a normative power (Gerrits 2009), rather than actions by Russia or China. Indeed, the debate on the self-perception of the EU and its legitimacy as a foreign actor have been central to the discussion on civilian and normative power. Scholars have made the point, that the notion of European normative power is caught in a central contradiction: the EU sees itself as having moved beyond the concept of nation-state sovereignty and having a 'post-national' legitimacy claim, yet only a concrete political order as found in its member states (MS) can provide the legitimacy that the EU needs in order to promote normative European power (Bickerton 2011). According to Manners, this contradiction can be resolved through the concept of normative power, which is different to Duchenes' civilian power approach. Sjursen argues that legitimacy can be located in the EU's contribution to cosmopolitan law. The following section will review these two concepts in greater detail.

Arguably, the contribution by Manners (2002) was most influential in reshaping the debate on normative European power. In regards to the legitimacy debate, Manners argument was that Europe's normative power should be understood as the result of its transformative impact on global politics (Bickerton 2011). Manners describes this in the following words:

'The creative efforts of the European integration process have changed what passes for 'normal' in world politics. Simply by existing as different in a world of states and the relations between them, the European Union changes the normality of 'international relations'. In this respect, the EU is a normative power: it changes the norms, standards and prescriptions of world politics away from the bounded expectations of state-centricity'. (Manners 2008).

This approach is in so far different from the concept of civilian power, as civilian power relies on the tenets laid out by Smith above in this chapter. Yet, these rely on state-centered assumptions of international relations. Manners on the other hand saw the EU as a promoter of norms which replace the state on a global level (Manners 2002). This is relevant as this concept has gone beyond mere academia and has been taken up by policy makers across the EU (Bickerton 2011). Bickerton quotes two former Presidents of the European Commission,

who put the notion of European normative power at the forefront. Jose Manuel Barroso said that 'the EU is one of the most important, if not the most important, normative powers in the world…It is in fact the EU that sets the standards for others much of the time' (Bickerton 2011, 28). The quote of Romano Prodi likewise shows how much relevance is attached to this concept: 'Only by ensuring sustainable global development can Europe guarantee its own strategic security' (Bickerton 2011, 28). This is noteworthy, as it shows how the concept of normative power can transcend into other policy areas and is actively connected to security. Until now, focus has been on development, human rights and environmental change, however it may also be applied to 'newer' areas, such as cyber security.

In order to further clarify the concept of normative power, Manners differentiates four steps: Ideational, principles, actions and impact (Manners 2009). Ideational means that it involves justification instead of physical force or material incentives. If this justification is to be successful, it must be built on coherent principles, which are seen as legitimate. Many of these principles draw their legitimacy from internationally recognized documents such as the UN Charter, the European Convention on Human Rights etc. Subsequently, action refers to the activities undertaken to promote these principles. Concepts such as persuasion, argumentation or blaming and shaming are important tools to act for such principles. Finally, impact should be ultimately envisaged through normative power. Manners sees partnerships 'impact of the promotion of principles may be the result of institutionalized relationships (…) whether multilateral or international (…)' (Manners 2009, 14). However, the author also recognizes that measuring the EU's impact in promoting principles is very difficult to examine. Citing some examples, he comes to the conclusion that partnerships and success in multilateral institutions, rather than EU unilateralism, is important 'when attempting to judge EU principles, actions and impact in any normatively sustainable way' (Manners 2009, 14). It is important to reiterate that these four steps are seen in an ideal, purely non-coercive and non-materialistic form but Manners recognizes that material incentives and physical force may sometimes also be used in order to achieve goals. However, focusing on normative power urges the EU to thoroughly justify these measures (Manners 2009).

Judging impact of EU normative power leads to the second point, in which legitimacy of such power may be found: the contribution to cosmopolitan law. Sjursen brings a refreshing criticism towards the notion of normative and civilian power, especially the idea of the EU as

a ‘force for good’ (Sjursen 2006). Manners claim however, is not so much in the difference between military and non-military powers and whether this may disqualify the EU as a civilian power, but rather that ‘the EU’s ability to shape conceptions of ‘normal’ need to be given much greater attention again’ (Manners 2002, 239). Recognizing this differentiation, Sjursen calls for a conceptual apparatus which is able to distinguish whether the EU can indeed be seen as normative, rather than merely self-interest driven and as such expressing ‘Eurocentric Imperialism’ (Sjursen 2006, 242). This is vital, as norms and values are perceived differently in different parts of the globe. Drawing a comparison to the US, which under Reagan promoted Western values globally out of a deep-rooted conviction that it is beneficial for the whole world, the scholar argues that merely promoting norms is just another form of power politics. As such, there should be more to normative power. Sjursen also returns to the question of the legitimacy of European power as this is baseline for successful norm promotion. Unlike Manners, who locates legitimacy in the EU’s post-national design, Sjursen calls for better analysis to what extend the EU’s foreign policies contribute to cosmopolitan law. The difference of cosmopolitan and international law lies in the subjects: Whilst international law is mainly preoccupied with states and/or other forms of polities, cosmopolitan law should protect individuals (Sjursen 2006). Only by contributing to cosmopolitan law, can the EU avoid debates about norm justification (i.e. why should a certain norm exist?) or norm application (i.e. what exactly does a norm prescribe?). These two parts of the norm debate provide most friction when promoting norms in a culturally fundamentally different environment. In cyber security this proves even more challenging, as cyber security covers a wide array of humanitarian, economic, social and national security topics and particular governance structure (autonomy from sovereign control and multi-stakeholder approach) (Finnemore and Hollis 2016).

Some of the criticisms around the concept of normative and civilian power have already been touched upon. The most prominent critique lies in the fact that the EU has begun to ‘militarize’ its foreign relations, most notably via the Common Security and Defense Policy (CSDP), which allows the EU to call upon military defense materials from its MS. After all, the claim that Americans are from Mars and Europeans from Venus (Kagan 2003), does not hold anymore, yet played an important role in Duchêne’s original argument. In essence then, this criticism calls into question the *distinctness* of European power. Gerrits sees the debate as a product of the Zeitgeist which was predominant after the demise of the Soviet Union (Gerrits

2009), in which a moment of liberal institutionalism and universalism were at their peak. As such, he sees that the debate has somewhat lost its relevance recently. Nevertheless, other authors have addressed this criticism by focusing not so much on the *sui generis* nature of European power, but rather the extend to which this kind of power still matters in today's rapidly changing world (Aggestam 2009).

Focusing on the points made by Aggestam, as well as Manners and Sjursen provides a conceptual framework for this thesis. This paper does not seek to reject or confirm the notion of European normative power, it rather looks for mechanisms under which current political action undertaken by the EU may be explained. Both Sjursen and Manners allude to the concept of the norm-life-cycle, by acknowledging that 'norms matter' (Wiener and Puetter 2009).

2.2. Norms Research in International Relations

To orient oneself in the broad field of norm research and to differentiate between different concepts is a difficult but indispensable task for successful norms research. Norms research has not been developed in a classical way through debates, but can be regarded as 'cluster formation at the same time' (Loges 2014). It has produced various definitions of norms. The focus is on the context of norms, their influence and their development (Finnemore and Sikkink 1998). Constructivist research could, however, agree on oneformula: 'Norms matter' (March and Olsen 1998).

Norms research makes it possible to recognize the underlying structure of actors' behavior. The classical definition of Finnermore and Sikkink defines norms as 'a standard of appropriate behavior for actors with a given identity' (Finnemore and Sikkink 1998). It is already suggested that norms are not universally valid, independent of the actors and their context. Norms are intersubjective variables, which are not arbitrarily transferable to situations and actors. A common identity is the prerequisite for the following definition: 'Norms are accepted, sanctioned prescriptions for, or prohibitions against, others' behavior, belief, or feeling - or else' (Wiener and Puetter 2009). In this context, rules and norms are distinguishable. They differ by the degree of their formalization: 'Rules and norms are distinguishable by how formal they are, norms being sufficiently informal that observers are

not always sure that they are rules until they see how other agents respond to them' (Onuf 1998). Here, intersubjectivity is emphasized. Only by the behavior of other actors vis-à-vis a norm is this also recognizable. As a result, behavior is judged to be appropriate or inappropriate. Engelkamp et al. define norms and actors' action as follows: 'Actors act according to a logic of appropriateness. They adopt intersubjective shared norms that are linked to specific identities and roles for actors. These identities activate specific notions of good and legitimate behavior, which in turn guide and shape social action '(Engelkamp, Glaab, and Renner 2012).

According to Loges, most of the studies of normative research are based on the following basic convictions: the reciprocal constitution of actors and structures, intersubjectivity and communicative process (Loges 2014, 9). The alternating constitution of the actor and structure is probably the most complex component. Constructivists assume that actors and structure are interrelated and mutually dependent. The assessment of the influence of one variable on the other is very difficult. Based on research pragmatism, results-oriented research will usually decide to focus on one of the two variables only (Loges 2014).

Actors act out of their embedding in their social structures. These serve as an interpretative framework for their actions and the interpretations of their environment. 'This social space of the individual shared sense is determined in an intersubjective way' (Loges 204, 146). Through the intersubjective anchoring of norms, holistic action becomes possible within this framework. Communicative process illustrates the importance of language for the identification of norms. 'Only through interaction processes is the social world constituted and reconstructed, to which norms also belong' (Loges 2014, 146). For this reason, the reciprocal structure of the actor and structure, as well as intersubjectivity, cannot be conceived without the communicative process. In particular, the nature of the discourse is crucial for the spread of norms. One of the most influential studies on norm research is the 'Norm Life Cycle' model by Sikkink and Finnemore, which conceptualizes the emergence of a norm, diffusion on an international level, to the internalization by the actors (Finnemore and Sikkink 1998). Normally, norm diffusion is carried out through so called 'norm entrepreneurs', who are actively involved in the dissemination of a norm and are in competition with other norm entrepreneurs (Finnemore and Sikkink 1998). Once the norm has reached the phase of internalization, the conflicts around the norm disappear. The absence of debates on the

validity of a norm serves as a gauge for the internalization of the norm. Without contestation around the norm, i.e. without public discourse, the norm is considered to be fully internalized, implemented and is located in its high phase, also called 'cascade' (Finnemore and Sikkink 1998). Norms often require a norm entrepreneur in order to become successful. Following Finnemore and Sikkink's argument, the norm entrepreneur plays an important role from the norm emergence to the cascade of a norm. The first stage, or emergence of a norm, is characterized by persuasion. Here, norm entrepreneurs attempt to convince a critical mass of states or other actors to embrace a new norm. The second stage, the beginning of the norm cascade sees the 'imitation' of the norm, as Finnemore and Sikkink call it (Finnemore and Sikkink 1998, 895), by other actors. The reasons for why a norm is imitated vary, but can usually be located in the wish for legitimization by states and pressure of other states. All these stages see active engagement of an actor pushing the norm through the life-cycle. This school of thought is also called 'the logic of appropriate behavior'. Norms are defined as variables which influence and guide the behavior of states and their actors. Prominent thinkers of this school are March and Olsen (2006), Finnemore and Sikkink (1998), as well as Katzenstein (1998) and Checkel (2001). According to this theory, norms are constitutive of the social structure in which actors operate. While the state, as a powerful actor within international relations, is never questioned in this way of thinking, it has been possible to explain the influence of social groups on international decisions (Wiener 2014). Therefore, this is also the 'conventional constructivist strand' of thinkers (Wiener 2014). March and Olsen define Logic of Appropriateness as 'rules are followed because they are seen as natural, rightful, expected, and legitimate. (...) Actors seek to fulfill the obligations encapsulated in a role, identity (...) Embedded in a social collectivity, they do what they see as appropriate for themselves in a specific type of situation' (March and Olsen 2006). By concentrating on the rules that shape human behavior, a blurry world can be explained, for rules and norms contain collective and individual roles, worldviews, rights and duties, and much more (March and Olsen 2006). Bastian Loges criticizes the question of causality (Loges 2014) within the logic of appropriateness. In his view, the assumption that norms are static bears the risk that no convincing causality can be found between acceptance or rejection of norms (Loges 2014). Loges finds this in a lack of context, which has not been sufficiently conceptualized, but is indispensable for a convincing causality. Instead, 'classical' causality dominates, apart from specific context conditions (Loges 2014, 11). 'It was first and foremost a question of deriving

theoretical concepts from research, or of examining concepts for empiricism. (...) The dynamics and process ability (...) ended with the research design for the analysis of norms '(ibid 2014). The contextual conditions find much more attention in later researches in order to conceptualize norms with their help. Since behavior towards norms is theorized dichotomously, behavior is categorized in observance and non-observance of a norm.

The 'logic of arguing', which has been conceptualized above all by the theorists such as Thomas Risse (2000) and Nicole Deitelhoff (2013), focuses on the behavior of states towards norms, especially the communication about the norm. Argumentation is used strategically to legitimize norms. Thomas Risse argues in the essay 'Let's argue': Communicative Action in World Politics' that there is a third way in international relations between instrumental rationalism and standardized behavior (Risse 2000) At the same time, Risse refers to Jürgen Habermas' theory of communicative action in which he assumes that actors must be prepared to be convinced of the better argument. This plays a special role for the constituent function of norms. They are not regulatory, since the logic of arguing allows actors to verify their respective norms. The fact that actors were involved in the better argument and were ready to be convinced changed their world view, their interests and even their identities (Risse 2000). The logic of arguing seeks to explore and explain how norms, in particular human rights norms, influence the politics of a state and how inversely the politics is influenced by them (Wiener 2014). Thomas Risse et al. propose a spiral model which shows how the internalization of human rights within the community of states varies (Risse 1999). In the spiral model strategies of blaming and shaming are also conceptualized to put pressure on states. This strategy of blaming and shaming is called a top-down instrument which offered much room for criticism. The use of pressure to bring about a normative change can lose its value as a convincing argument and as a result dissolves the strict reading of Habermas.

Taking the standard definition of 'norms as a standard of appropriate behavior for actors with a given identity', Finnemore and Hollis dissect this definition in four conceptual pieces: Identity, behavior, propriety and collective expectations (Finnemore and Hollis 2016). In their analysis, (1) Identity refers to the group to which the norms apply, (2) behavior prescribes the specific actions required by the norm and its nature (regulative, constitutive etc.), (3) propriety suggests the basis on which norms label behavior as appropriate or inappropriate (in other words the 'oughtness' of normative claims) and finally the (4) collective

expectations refer to the social character of norms, the fact that norms are shared understandings and not unilateral orders (Finnemore and Hollis 2016). Such conceptual pieces facilitate research in the norms debate, as they provide clear-cut evidence to assess whether norm building is successful.

As is evident, it is common for researchers in social constructivism to focus on the 'process' of norm building, rather than the impact. This also holds true for norms in cyber security. Finnemore and Hollis find the challenge in overcoming 'the view of cybernorms as the fixed products of negotiation, locked-in agreements that can settle negotiations' (Finnemore and Hollis 2016, 477). Based on the literature review of both European normative power and norms research in international relations, this thesis seeks to analyze whether the EU is acting as a norm entrepreneur in building norms for a shared understanding of cyber security. The tool utilized by the EU are cyber diplomacy in key-partnerships, clearly aimed at persuading great powers to adopt similar definitions and norms of cyber security. Currently, it appears as if the norm still finds itself in the first stage of the norm life cycle, wherein the EU acts in persuading other actors to adopt a common understanding of the issue at stake.

2.3. Cyber Security and Cybercrime

Before assessing how the EU acts a norm entrepreneur, it is useful to define the issues of cyber security and cybercrime. Much of the work done by the EU is to work towards a globally shared understanding of cyber norms. Determining what cyber security entails deserves a research thesis in its own right. Yet, any research treating cyber security must be clear in its definition of cyber security. One can identify two broad categories of cyber threats: cyber security and cybercrime. Whilst the first dimension involves political motives such as power maximization and creation of advantages and disadvantages or disruption (eg. terrorism) (Sliwinski 2014), cybercrime is targeted at private citizens and businesses without a political agenda, marked by a transnational nature. The perpetrators rather seek to obtain data to maximize profits. The problem may seem rather novel to outside observers, rendering it more difficult to identify a widely - shared definition. Warner traces the development of the understanding of cyber in general and cyber security in particular back to the 1970s (Warner 2012). His research is valuable, as decisions and debates in the past still shed their light on our

current understanding of cyber security. The baseline is apparent: all security serves the protection against various threats, posed by inherent vulnerabilities. Authors have stressed that cyber security is not to be confused with information security (von Solms and van Niekerk 2013). Although these terms are often used interchangeably, the key difference lies in the subject of protection. Whilst information security is the protection of information, an asset, from harm resulting out of vulnerabilities, cyber security is not only the protection of the cyberspace itself, but likewise the protection of those that act within cyberspace (mainly natural persons) and can be reached via cyberspace (von Solms and van Niekerk 2013). Such lack of terminological precision in the wider literature complicates the research. This lack of widely accepted definition has sparked a whole range of academic papers. The most important finding of the research is that 'the way in which the issue is framed influences what constitutes a threat as well as what measures are needed and justified' (Choucri, Daw Elbait, and Madnick 2012). This problem is aggravated in the setting of multilateral institutions, as different members have differing definitions. In the EU, the Netherlands and Germany see cyber security as a homeland security issue, whereas Denmark defines the responsibility under the Ministry of Defense and as such producing differing threat responses (Pawlak 2016b). As an illustration of the lack of conceptual clarity, the Dutch Ministry of Security and Justice defines cyber security as follows:

> *'Cyber security is freedom from danger or damage due to the disruption, breakdown, or misuse of ICT. The danger or damage resulting from disruption, breakdown, or misuse may consist of limitations to the availability or reliability of ICT, breaches of the confidentiality of information stored on ICT media, or damage to the integrity of that information' (*Boeke et al. 2016).

As is evident, this definition is closer to information security, rather than cyber security as it omits the human dimension. The EU institutions have not issued a definition of cyber security. However, the European Union Agency for Network and Information Security (ENISA), the main EU body for cyber security, has a working definition of cyber security which is relevant for this thesis:

> *'the protection of information, information systems, infrastructure and the applications that run on top of it from those threats that are associated with a globally connected environment'* (Helmbrecht, Purser, and Ritter Klejnstrup 2012)

Importantly, the EU here takes into consideration the physical infrastructure of ICT systems which is vital for a coherent security strategy. After all, the best cyber security system is useless if the physical infrastructure can be compromised. It becomes apparent, that cyber security remains a contested area internationally. In realist terms, why would another state give up the possibility to conduct cyber espionage or sabotage, if it may further its gains and obtain an advantage?

Cybercrime however, might be more conducive to international regulation as states suffer equally from it. According to experts, in 2012 the cost of cybercrime has been estimated at USD 388 billion globally. That number is likely to have increased dramatically. In the EU in 2010, nearly 73% had an internet connection at home and 36% of European citizens used internet banking (European Commission 2012). The European Commission defines cybercrime as:

Cybercrime consists of criminal acts that are committed online by using electronic communications networks and information systems. It is a borderless problem that can be classified in three broad definitions:

1. *Crimes specific to the Internet, such as attacks against information systems or phishing (e.g. fake bank websites to solicit passwords enabling access to victims' bank accounts).*
2. *Online fraud and forgery. Large-scale fraud can be committed online through instruments such as identity theft, phishing, spam and malicious code.*
3. *Illegal online content, including child sexual abuse material, incitement to racial hatred, incitement to terrorist acts and glorification of violence, terrorism, racism and xenophobia.* (European Commission 2016a)

In this definition, the European Commission explicitly recognizes the transnational nature of cybercrime. However, the institutional set-up still reflects the pillar system of policy separation in which Directorate General (DG) Home leads on criminal elements and DG Connect on network security and resilience. Having established the definitions and differences of cyber security and cybercrime, the next section will analyze to what extend the EU acts as a cyber security agent and whether its initiatives in regulating the cyber domain have been successful.

2.3.1. The EU as a Cyber Security Agent

Mapping cyber security in the EU is vital to understanding the organization and management of threats and responses. There are several dimensions to cyber security, most notably the civilian side, such as public-private partnerships and policing as well as the military side. This section outlines some of the steps taken by the European institutions and demonstrates that these serve as both internal and external norm building. It is noteworthy that the EU has only introduced a cyber security strategy fairly recently in 2013, the 'Cyber Security Strategy: Open, Safe and Secure'. The prime responsibility however for organizing effective cyber security lies with the MS. The strategy pursues five strategic priorities, among them, 'developing cyber defense policies and capabilities under the CSDP' and the development of a 'coherent international cyberspace policy' for the EU. The more external norm building aspect of promoting a globally shared understanding of cyber security falls in the competence of the Common Foreign and Security Policy (CFSP).

The military widely regards cyber as the 'fifth domain', next to the traditional four domains sea, land, air and space. In the EU, military cooperation is organized under the CSDP. For conventional military missions, the EU does not possess standing military forces and capabilities, it is wholly dependent on its MS to contribute material and personnel to missions. The same holds true for European cyber capabilities. The main European body organizing and coordinating such capabilities is the European Defense Agency (EDA). As at the moment cyber security capabilities vary greatly between MS, it is EDA's task to level these differences as much as possible (Viewpoints 2017).

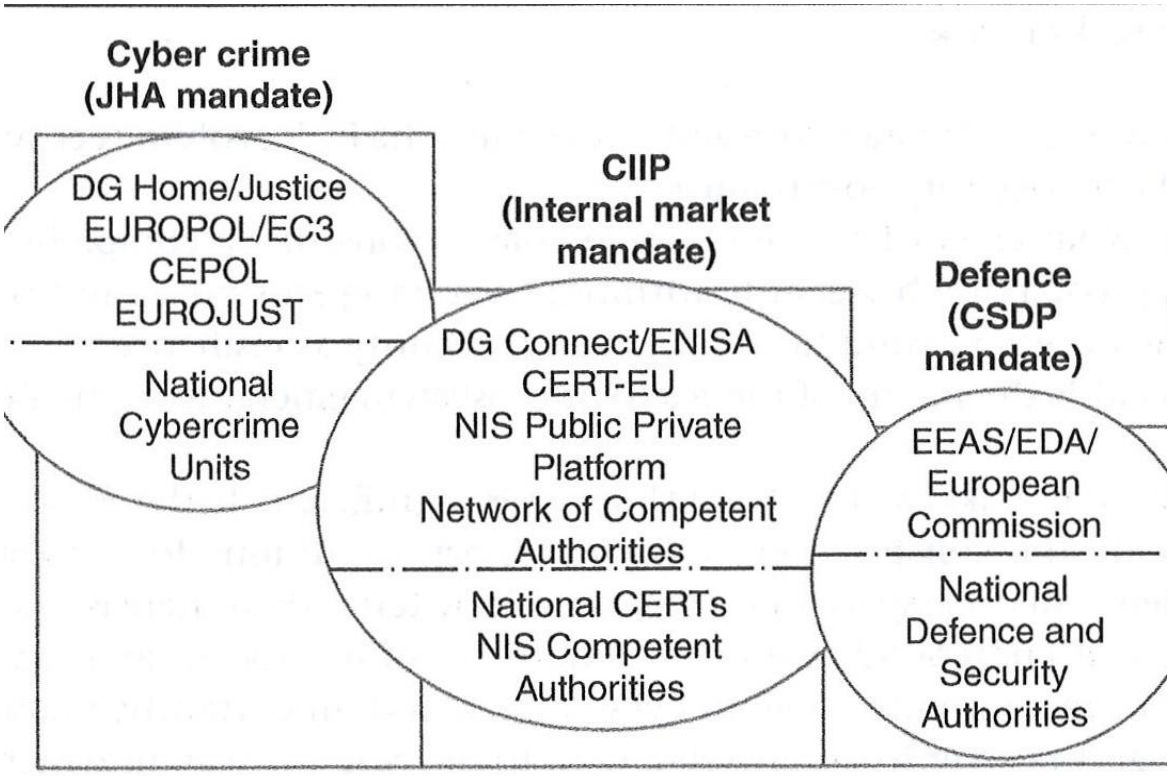

Figure 1. The central pillars of the EU Cybersecurity strategy (Christou 2016, 3)

Figure 1 illustrates how competencies are divided within the EU as well as the MS.

A milestone was reached in 2013, when the EU published its cyber security strategy. The EU seeks to promote a 'coherent international cyberspace policy' as one of its key five priorities (Renard 2014). This is supplemented by the Council Conclusions on Cyber Diplomacy which clearly recognize that:

'*cyber security, the promotion and protection of human rights in cyberspace, the application of existing international law, rule of law and norms of behavior in cyberspace, Internet governance, the digital economy, cyber capacity building and development, and strategic cyber relations offer significant opportunities, but also pose continuously evolving challenges for EU external policies, including the CFSP'* (Council of the European Union 2015)

It becomes evident that the EU institutions have recognized the need for a streamlined approach to cyber security. This approach is two-fold as it focuses both on the internal and external dimension of the EU. By mentioning the CFSP however, the EU clearly identifies the importance of dialogue with external actors. As Christou puts it: 'Fostering trust and security in cyberspace is not an option for the EU, it is a requirement' (Christou 2016). Both cybercrime

and cyber security have two dimensions to The EU's approach: an economic logic and a defense logic (Christou 2016). The economic logic motivates businesses and actors to incentivize and stimulate a secure information society for all to minimize losses, whilst the defense logic is derived from protecting critical infrastructure against terrorist and third state attacks.

As shown in Figure 1, cybercrime is under the mandate of the Justice and Home Affairs Council (JHA), which is part of the Council of the EU. The most notable internal achievement is the European Cybercrime Centre (EC3), which is part of Europol. Establishing this center was mainly driven by the Internal Security Strategy (Fahey 2014). The purpose of EC3 is to strengthen a transnational law enforcement response to cybercrime, taking a three-pillar approach, consisting of forensics, strategy and operations (Europol 2017). The EC3 is considered as a central node in fighting cybercrime by pooling expertise, supporting investigations, promoting EU-wide solutions and raising awareness (Christou 2016). However, the EU still faces challenges, such as jurisdictional boundaries, insufficient intelligence-sharing capabilities, technical difficulties in tracing the origins of cybercrime perpetrators, disparate investigative and forensic capacities, scarcity of trained staff, and inconsistent cooperation with other stakeholders responsible for cyber security (European Commission 2012). The external driver for cybercrime policy has been the European Convention on Cybercrime of the Council of Europe, commonly known as the Budapest Convention. The Budapest Convention is the only binding international instrument on this issue, 'serving as a guideline for any country developing comprehensive national legislation and as framework for international cooperation between State Parties to this treaty' (Council of Europe 2014). The importance of this legal document becomes apparent when taking into account that so far, no legal definition for cybercrime can be located in primary or secondary EU law. Instead, the content of the Budapest convention forms the basis for both internal and external rule-making (Fahey 2014). It is therefore regarded as 'a major advance toward creating a common judicial area in cyber issues' (Bendiek 2014, 10). The convention is also open to non-member states of the Council of Europe. However, the Budapest Convention has also drawn criticisms regarding its infringement on sovereignty. More specifically, Article 32 allows local police authorities to access servers located in another country's jurisdiction without seeking approval of relevant authorities (Shalini 2016). The idea behind this article is to enable quick securing of electronic evidence. The issue of sovereignty infringement has been addressed and countered by the

Cybercrime Convention Committee, a body to regulate arising issues, in a guidance note on Article 32 (Shalini 2016).

One could argue that the EU is not only a norm entrepreneur towards third country states but also internally. The different levels of cyber security capabilities within the EU called for the need to build a coherent set of values and norms to be complied with in order to construct a culture of cyber security in all MS. To that end, ENISA was established. This move created a center which would recommend and provide advice on good practices in information security. Furthermore, it assists in collaboration between relevant actors and supports MS in implementing European legislation on cyber security into national law. The link between internal and external European rule-making on cyber security and cybercrime is evident. The EU Internal Security Strategy explicitly mentions the success and effectiveness of the EU-US cybercrime and Cyber Security Working Group (WGCC). The Cyber Security Strategy also references the US as the EU's most important partner in rule-making (Fahey 2014). Fahey (2014) demonstrates that there is a strong dichotomy in internal and external EU security regulations with regards to cyber issues. However, whilst the EU is rather ambitious in its goals for external norm construction, setting out to create a global cyber regime, as the WGCC goals suggest, the internal dimension of rule-making is rather modest. Instead, the internal dimension appears less ambitious in its failure to regulate holistically, transparently and systematically (Fahey 2014). Yet, not only the EU is an important norm setter in regards to cyber security. For example, Crandall and Allan show how Estonia functioned as a norm entrepreneur in raising and dramatizing cyber security issues (Crandall and Allan 2015). Their platform was not so much the European institutions but rather NATO. Operating through the institutional setting of NATO, Estonia has managed to change the perception of cyberattacks to such a degree that nations may now invoke Article 5 when facing a cyberattack. However, the research also demonstrates that choosing NATO as a platform has certain impediments, for example leaving out Russia of the norm emergence discussion and therefore hindering a widely shared understanding of such cyber norms (Crandall and Allan 2015).

When discussing the EU as a cyber security agent, the question arises as to how the European civilian power approach falls into this category. As the first section discusses, a more defensive and less offensive nature of the EU has been at the onset of that discussion, leading to the term civilian power. Unlike multilateral institutions such as NATO, the EU can be

regarded as a somewhat defensive/reactive actor in cyber (Sliwinski 2014). Evidently, the EU institutions have been a valuable target with at least one successful attack in 2011 when emissions worth 30€ million had been stolen from the EUs Emissions Trading Scheme (House of Lords 2011). Similar to national Computer Emergency Response Teams (CERTs), the EU has established its own permanent CERT-EU. According to the CERT-EU mission statement it is responsible for the following:

> *CERT-EU's mission is to support the European Institutions to protect themselves against intentional and malicious attacks that would hamper the integrity of their IT assets and harm the interests of the EU. The scope of CERT-EU's activities covers prevention, detection, response and recovery* (CERT-EU 2013).

Manifestly, the role of European cyber security teams is focused more on building resilience rather than acting proactively. Whilst recognizing that the main responsibility lies with the MS, the Council conclusions on countering hybrid threats of April 2016 underline the need to mobilize EU instruments to counter these threats more effectively (Council of the European Union 2016a). As mentioned above, other multilateral institutions have taken more radical steps such as NATO in extending Article 5 to the cyber realm. Furthermore, leaders affirmed at the NATO summit in Warsaw 2016 the readiness to counter hybrid threats, such as cyber warfare, as part of collective defense and the willingness to assist an ally at any stage of a hybrid campaign (Pawlak 2017). Compared to other multilateral institutions, therefore, it becomes clear that the EU has kept its civilian status in the cyber realm by constructing a resilient and protected network, rather than seeking to develop offensive capabilities towards other actors.

Some authors, however, see the EU as a failed cyber security agent (Sliwinski 2014). This is partly due to the unique structure of the EU as an institution *sui generis* but also the lack of a common, clearly defined foreign strategy and common notion of cyber security. Embedding cyber security into the concept of a soft power or normative power approach could thus facilitate the formulation of a comprehensive strategy and give guidance to MS. Concentrating on the defensive side, as a normative power, bears the risk to not be able to influence fully the myriad of actors and phenomena in cyber space (Sliwinski 2014). Whilst the main argument of this thesis focuses on the 'offline' diplomatic dimension – namely partnerships and treaties - the EU lacks a presence in certain online areas. Furthermore, the nature of

European free markets limits the influence of European decision making decisively. Many public goods, such as telecommunication infrastructures are owned by private actors, leading the EU to having to narrowly define the responses of private actors in case of a security breach. Differences in national legislation also pose challenges. Sliwinski sees the answer to this in a further 'Brusselization', a possible further transfer of rights to the EU, which is opposed by many MS (Sliwinski 2014, 481). Lastly, as has already been mentioned in this section, the disconnect between internal and external norm building is troubling to some authors. Many proposed actions have been deemed ineffective and disproportionate, especially in regards to cybercrime, whilst externally the actions by the EU have not yet wielded much success (Fahey 2014). It is safe to conclude that a cyber regime is still under construction within the EU and that it will face challenges in the years to come.

2.3.2. Cyber Diplomacy

Cyber diplomacy is defined as the use of traditional diplomatic tools to address global cyber issues, such as cybercrime, cyber security, cyber defense and internet governance. Other authors situate this in the broader concept of digital diplomacy (Hocking and Melissen 2015). Whilst digital diplomacy changes the nature of diplomacy in many ways, such as changing hierarchies and new ways of communication (WhatsApp etc.), cyber diplomacy is linked to what Hocking and Melissen call 'cyber agendas', in essence building a framework for appropriate behavior in cyberspace. The definition indicates that the term cyber diplomacy is more of a buzzword than an actual fully defined concept with distinct features. This is also supported by other authors, who recognize that cyber diplomacy is novel as it encapsulates an area, which has so far not been considered as work for diplomats, but nonetheless requiring 'old school statecraft' such as treaties and the development of (soft) international law (Tirrmaa-Klaar 2013). Important for cyber diplomats is therefore to quickly learn 'how to speak cyber' and to obtain a sound knowledge of topics such as information technology (ICT) developments, computer and network security, internet governance, international security, cybercrime and cyber intelligence (Tirrmaa-Klaar 2013). Difficulties in finding a global cyber diplomacy definition is closely connected to an international disagreement on the terminology of cyber security, aggression in cyberspace and cyber weapons (Danca 2015). To that end, the

Organization of Security and Cooperation in Europe (OSCE) is in the process of developing a glossary of specific terms in partnership with all participating states (OSCE 2013). Even if the notion of cyber diplomacy is still somewhat contested, it is apparent that the most relevant issue lies in regulating international cyber behavior. As national decisions on how to act in cyberspace have strong international implications, the notion of cyber diplomacy is especially important to foster a culture of international commitment and collaboration, including private stake-holders (Danca 2015).

However, as cyber diplomacy will grow in relevance, certain distinctions will develop. One of these can already be observed today, more specifically the multi-stakeholder approach. In the EU Commission report 'Europe's role in shaping the future of Internet governance', this is explicitly mentioned (European Commission 2014b). As such, cyber diplomacy is a move away from state centered governance to the inclusion of many more actors, such as NGOs, businesses and multilateral organizations. In this regard the EU Commission describes itself as an 'honest broker' in shaping internet governance globally (Renard 2014). The term honest broker can also be translated to norm entrepreneur, as it seeks to promote norms in cyberspace and actively contribute to the formulation of these norms. In order to achieve this, the EU has established several strategic partnerships with countries around the globe. Some of these partnerships, for example with the US, are already quite developed whilst others (China and Russia) lack greater in-depth cooperation. As has been discussed in the previous chapter, EU norm building is marked by an internal and external dichotomous reliance on these norms. Both dimensions feed into the formulation of cyber norms.

Smith et al. identify three different levels of purpose for strategic European diplomacy: reflexive, relational and structural (M. H. Smith, Keukeleire, and Vanhoonacker 2016). These can also be witnessed in the key partnerships. The reflexive level refers to 'integrative' and 'positional' strategic partnerships; they are integrative as they promote a coherent EU foreign policy and positional in the sense that they affirm the global standing of the EU as a global actor. The integrative approach is supported by the literature on European normative power as it supports a foreign policy identity and legitimacy building through these partnerships. Smith et al. also note that for the relational level, 'strategic partnerships are means of managing relationships with key partners or in key issue areas which are important to the international life of the union' (M. H. Smith, Keukeleire, and Vanhoonacker 2016, 5). Solving

global problems alone is not feasible as the Council of the EU recognizes (Council of the European Union 2008), therefore such partnerships must be addressed in cooperation on the basis of mutual interests and benefits. Renard notes that the relational aspect is the most salient one, as in some cases the main interest of engagement in the partnerships lies in the process of socialization, more than in specific outcomes (Renard 2014). Finally, the structural level refers to the strategic partnerships as instrument to promote and shape a more effective multilateral system (Renard 2014). This is also confirmed by the Council of the EU, which labels it as 'partnerships for effective multilateralism' (Council of the European Union 2008).

As a summary, cyber diplomacy is not a brand-new phenomenon. It rather addresses the role of diplomacy in an environment which is less well-regulated internationally and more contested than other areas. Yet, the term cyber diplomacy is misleading as it implies a change in the nature of diplomacy. The concept of digital diplomacy as described by Hocking and Melissen captures the change that cyberspace has brought to the nature of diplomacy. Nonetheless, the concept of cyber diplomacy is the tool to act as a norm entrepreneur. The chapter on norms research shows that building norms does not happen in a vacuum, instead specific social environments and cultural backgrounds constitute the basis for norm promotion. As such, the tool of cyber diplomacy might be the right fit to respond to these changing environments, as they allow tailored approaches to the needs of different actors.

3. Research Design

3.1. Research Question and Sub Questions

Following the definitions and theoretical framework, several questions for the thesis arise. To reiterate, the research question is: *How is the European Union as a normative power promoting global norms of cyber security?*

As the chapter on norm research has shown, the norm life cycle goes through various stages before norms become internalized. In order to influence other actors' behavior towards norms, communication is essential. This leads to hypothesis 1:

H_1 : *the closer the working relationships are that the EU has with a non- member state on the topic of cyber, the more likely will the state adopt some of the cyber norms promulgated by the EU.*

To explore hypothesis one, it is necessary to assess the extent to which the EU collaborates with specific partners in the area of cyber. Here, the independent variable is the existing relationship between two actors. The dependent variable is the impact of cyber diplomacy, which is the tool to specifically address cyber challenges within these partnerships.

This will be done by assessing documents issued by the EU and respective partners between 2013 and 2017. This timeframe has been chosen as in 2013 the European Cybersecurity strategy had been revealed and cyber issues have since been taken up by the EEAS. As the thesis is relying on openly accessible sources, these documents are mainly press reports, joint statements and fact sheets, published by the EEAS. The research also compares cyber security strategy definitions prior and after the partnerships. This will give an indication whether the partnerships had an impact and whether the values promulge stated by the EU are reflected in new strategies. As the EU has produced reports and strategies on its efforts to promote internet governance, as well as published documents of the strategic partnerships, it will be possible to trace whether much of the promulgated values and norms found their way into these documents and partnerships.

As a sub hypothesis, to examine the influence of cyber diplomacy with the countries' cyber security strategy as indicator, hypothesis 1a posits that:

H_{1a}: *The more a cyber security strategy has changed towards a value-driven approach since the EU partnership, the more successful the EU acts as norm entrepreneur.*

This reflects the norms and values promoted by the EU in its efforts to strengthen internet governance. If a country has changed its cyber security strategy in a way that reflects to certain degree the EU's vision, we can posit that the EU has in fact had an influence.

The EU has chosen cyber diplomacy as a tool to promote norm formulation. Further, the section on cyber diplomacy lays out which purpose strategic partnerships fulfill for European foreign policy, which will be assessed in the case studies. Lastly, the section on cyber security has cited the Budapest Convention, the most important international agreement on

cybercrime. The EU seeks to promote signature and ratification of this agreement by third party states. These components lead to the second hypothesis:

H_2: *The more the EU is successful in promoting global cyber norms based on cyber diplomacy, the more it can be considered to be a norm entrepreneur*

The main independent variable to explore the validity of hypothesis two is cyber diplomacy. The research posits that the extend of cyber diplomacy contributes to the EU as a normative power. By utilizing cyber diplomacy, the EU acts as norm entrepreneur. To assess the intensity of cyber diplomacy, the research explores the development of the EU's use of cyber strategies in third states, for example to get more state signatories for relevant cyber treaties (such as the Budapest Convention). Furthermore, independent think tank reports will serve as a counterweight to critically reflect how successful such partnerships have been.

3.2. Case Selection

The cases to explore whether the EU has been successful as a norm entrepreneur include three strategic partnerships. The cases scrutinized are the partnerships EU–US, EU-India and EU-Russia. These three cases represent three different degrees of deepened partnerships. Whilst the EU and US have close working relationships on this topic, EU and India have a less ambitious partnership. EU and Russia have a limited cooperation in regards to a partnership, as the EU does not fully trust Russia and to some degree sees Russia as 'part of the problem, not the solution' (Renard 2014). However, the EU is seeking to build mutual trust, especially in the area of cybercrime.

The cases have been selected on a most similar system design basis (MSSD). MSSD seek to explain reasons for variance in the dependent variable (George and Bennett 2004). The EU has bilateral relationships with all three actors in one form or another, which represents the independent variable. Furthermore, cyber diplomacy is used in all three cases, to a lesser degree in Russia, representing the dependent variable. The thesis therefore seeks to explore how the outcomes of these relationships differ with regards to the construction on mutually recognized cyber norms by means of cyber diplomacy.

These cases allow for a diverse range of data to be collected, as results between all three cases will be different in terms of successfulness and the scope of strategic partnerships. As such, these cases allow to see how much influence the EU can exert vis-à-vis other great powers and whether it can be considered a norm entrepreneur in the cyber domain.

3.3. Content Analysis

Content Analysis will be mainly based on documents to scrutinize the EUs conceptualization of cyber security. This includes proposed directives, summit documents, reports and speeches. Bowen specifies that qualitative document analysis is often used in combination with other qualitative research methods (Bowen 2009) such as interviews. It mainly serves to support the argument, as one evidence source is often not deemed acceptable (Bowen 2009). Bowen also lists a number of advantages to document research which hold true for my personal research situation. Accordingly, document analysis allows for availability, efficiency, cost effectiveness, lack of obtrusion and reactivity, great detail and stability.

Specific attention in the document analysis will be paid to thematic analysis. This is defined as follows: 'Thematic analysis is a form of pattern recognition within the data, with emerging themes becoming the categories for analysis' (Bowen 2009, 32). The method of content analysis is further defined as 'a research technique for making replicable and valid inferences from data to their context' (Krippendorff 1980). This includes coding textual units into conceptual categories. Hsieh and Shannon also suggest that content analysis may serve to expand existing theories by better understanding the relationships between variables (Hsieh and Shannon 2005).

The strategic partnerships provide for documents to be scrutinized. In this case, it will be possible to scrutinize what the EU posits in its declarations, speeches, and cyber strategy and how many of these terms and meanings can be found back in the actual partnership documents. Thus, content analysis as a form of qualitative research allows to assess whether the EU is indeed acting as a norm entrepreneur.

As the section on norms research demonstrates, the process of norm formulation is of special interest to scrutinize whether a norm is accepted. This paper will rather look at tangible outcomes, such as agreements and public utterances of acceptance or non-acceptance by the countries in question. However, it will also take into consideration to what degree the EU has started to integrate specific cyber issues into agreements and as such bringing the topic of cyber to the top of the agenda. This is similar to the work of Crandall and Allan, who specifically looked at the content and frequency of speeches by the Estonian Government in order to bring the topic of cyber security to the top of the agenda.

3.4. Data Analysis

As the sections in the theoretical framework laid out, there are two specific approaches which will be used in this thesis. The first is the four pieces' approach (Identity, behavior prescription, and collective expectations) one used by Finnemore and Hollis, in order to examine how the cyber norms as formulated in the key partnerships meet these criteria. This method allows to make conclusions about the quality of the norms. The second approach focuses on the tools that the EU uses, more specifically its relationships. Smith et al. defined three different types of relationships (reflexive, relational and structural) (H. Smith 2002), which demonstrate the nature of the relationship and the subsequent results. Linking these two approaches together in the data analysis allows for deeper understanding of how the EU acts as a norm entrepreneur.

In order to compare the case studies, the analysis of the case studies will follow the same pattern. First, the existing partnership, both bilateral and on a multilateral level on cyber will be mapped and the intensity of these assessed. Secondly, the relation will be assessed to lastly analyze in which way and whether the EU has acted as a norm entrepreneur. To that end, the definition of cyber security will be compared to before and after the agreement. Thirdly, the section assesses how the partnerships address the issue of cybercrime.

The researcher used data out of official joint statements of the European Commission and the case country, further speeches by European Commissioners and directors on the topic of cyber, as well as fact sheets and press statements by the EEAS and secondary literature such as think tank reports were reviewed. In order to analyze the content of these documents,

specific attention was paid to statements which discussed norms and cyber in the same document or speech. Further, in order to analyze the understanding of cyber norms within the case countries, the cyber strategies were reviewed (or translations thereof) which was supplemented with the national security strategy in the case of Russia and the US.

In total, 3 speeches are cited directly in this research, whilst 7 were reviewed in total. Additionally, 4 press releases by the European Commission and 2 joint statements (the most recent) were analyzed. Further, 4 cyber security strategies and 2 national security strategies were examined. To create a broader understanding, the research strongly rests on various secondary literature to complete missing information.

3.5. Limitations

The study has several limitations. As discussed above, norms research often takes into account the public discourse about norms to analyze whether these norms have been fully internalized. For scope and language reasons, this will not be done in this thesis. This paper is interested into investigating to which degree the EU positions itself as a norm entrepreneur, rather than the effectiveness of these actions. As such, the novelty of the issues does not allow to declare without doubt to which extend subscription to a norm promulgated by the EU is merely a lip-service by other states or whether they have internalized the norm. Furthermore, the question of causality cannot be answered completely in this thesis. It may be able to show a link between the variables. The classified nature of the topic in question leads the researcher to rely on openly accessible sources, which might sometimes omit components that might lead to different conclusions.

4. Case Studies

4.1. EU-USA

4.1.1. Mapping Cyber Relations

The USA are by far the most important partner for the EU in regards to regulating cyber space internationally. This is largely due to the fact that the threat landscape is very similar, however differences remain in legal regulations and technical standards (van der Meulen, Jo,

and Soesanto 2015). Both the EU and US attract cyber criminals due to the financial power, bandwidth consistency and high number of Internet Service Providers (ISP). The most notable product of bilateral cooperation is the EU-US Working Group on Cybersecurity and Cybercrime (WGCC). It represents the 'first major transatlantic cooperation in security since a decade' (Fahey 2014, 55) and was established after the EU-US Summit in 2010. The WGCC features four expert sub-groups which focus on cyber incident management, public-private partnerships, awareness raising and cybercrime. Further to that, the EC3 and US Law Enforcement have pledged further cooperation order to address cybercrime effectively as well as having launched The Global Alliance against Child Sexual Abuse Online together, in which 53 other countries have committed voluntarily to combat online child sexual abuse (European External Action Service 2014). In 2013, the EU Commissioner for Home Affairs Cecilia Malmström recognized that there is no stronger partner for the EU in jointly combatting cybercrime and fostering cyber security on both the private and public level (European Commission 2017). Similarly, the partnership is singled out in the Cyber Security Strategy as 'particularly important' (European Commission 2013, 15). Both actors have obliged themselves to promote the signature and ratification of the legally binding Budapest Convention. This is in line with the European commitment to work towards a transnational legal framework. Taken all together, EU-US cooperation provides a dense institutional fabric to address issues arising from cyber activity.

However, cooperation on cyber issues also faces several challenges. Most importantly, the NSA spying scandal, or Snowden affair, have brought mistrust forward. The affair demonstrated that the US is willing to utilize its global cyber power also in allied states, even towards heads of states and prime ministers. A particularly contested area is the question of private citizens' data. On October 6, 2015, the European Court of Justice (ECJ) struck down the Safe Harbor Law, which allowed American companies with European branches to store user data on American servers (Kegel 2016). This is due to the fact that in European Law, privacy rights are regarded as a human right, whereas the US considers data protection to be a consumer protection law.

4.1.2. Norms Assessment

The identity of a norm refers to the group to which norms apply, more particularly whether they apply to individuals, particular states or larger socially constructed groups

(bankers, lawyers, multilateral institutions etc.) (Finnemore and Hollis 2016). The Cybersecurity Strategy of the US Department of Defense sees three main activities to further cyber norms: (1) enhance inter-agency cooperation, (2) building bridges to the private sector and (3) building alliances, coalitions and partnerships abroad (Department of Defense 2015). Both the US and the EU share the perception of cyber norms as a multi-stakeholder approach, in which various sectors, private and public, ought to be included in regulation of the internet. The Department of Homeland Security on the other hand puts emphasis on securing federal government cyberspace access, as it often administers critical infrastructures (Bush 2003).

Behavior refers to the specific actions required by the norm of the community (Finnemore and Hollis 2016). Both the EU and US reaffirm in their joint statements that the same right of freedom of expression and the right to be free from arbitrary and unlawful interference must be uphold offline and online (European External Action Service 2014). In regards to cyber norms, many norms are regulative in character, prescribing, permitting or prohibiting certain behaviors. This also includes creating institutions. In regards to internet governance, both actors stress enhancing the accountability of the Internet Corporation for Assigned Names and Numbers (ICANN) (European External Action Service 2014). ICANN coordinates the unique indicators of computers globally, so that these can be identified. However, legally, ICANN is bound to Californian law and thus under US control. By pushing for the multi-stakeholder approach, the European Commission seeks to terminate American stewardship over the internet (Renard 2014).

Propriety refers to the basis on which norms label behavior as appropriate or inappropriate (Finnemore and Hollis 2016). The basis for cybercrime cooperation in EU-US relations can be found in the Budapest Convention, which both actors promote, and represents a clear legal definition for cybercrime. Similarly, the WGCC creates joint norms on cyber security and appropriate behavior as norms are a social construct. The EU-US dialogue indeed seeks to foster such norms by conducting joint table-top exercises and holding joint private-public workshops. As Finnemore and Hollis note, behavior by professional individuals in such joint exercises has a great impact on creating such norms, which later can be sought to be implemented into law (Finnemore and Hollis 2016).

Finally, collective expectation refers to the social and intersubjective character of norms (Finnemore and Hollis 2016). This is a somewhat contested area in EU-US relations. In regard to cybercrime, the collective expectation is met via the joint work of the US-Law enforcement and the EC3. Yet, regarding cyber espionage, the Snowden affair has demonstrated to European capitals that the US is willing to spy on close allies. It is therefore doubtful whether statements to refrain from such actions are actually sincere or merely a lip service. A similar issue is the use of offensive cyber weapons. Whilst the EU institutions are not (officially) developing any such weapons, the US cyber security clearly states that it reserves the right to respond appropriately in case of a cyber attack or to conduct preemptive strikes as the Stuxnet virus has demonstrated (Department of Defense 2015).

As a preliminary summary, the EU and US widely share the norms on cyber security. The joint statements of the cyber dialogue as well as the US cyber strategy share a similar conception of norms of cyber security and cybercrime, substantiated by a thick fabric of sharing of best practices, working groups and joint exercises. Assessing the quality of the norms, one may conclude that the issues which are jointly addressed are regarded similarly by the EU and the US. However, contentious areas such as the question of data protection are so far left out of the joint statements.

4.1.3. Relation Assessment

When assessing the EU-USA relationship following Smith's et al. definition, it appears as a reflexive relationship (M. H. Smith, Keukeleire, and Vanhoonacker 2016). As noted before, the EU-US cyber partnership bears particular importance for the formulation of the internal cyber security strategy of the EU. In this sense, the EU-US partnership fulfills an integrative role as it provides the EU with a narrative for more coherence and cohesion in the EU's foreign policy. As a norm entrepreneur, the EU sees this relationship as important since it gives legitimacy to the EU's claims and visions about cyber security. As the section on European normative power laid out, the EU is lacking legitimacy in its foreign policy endeavors. Partnering with one of the most important actors and the greatest global power, gives the EU a claim to legitimacy. After all, the US could have chosen to only conclude partnerships on a bilateral level with European MS, rather than the EU institutions. By enabling close working relationships on a sensitive topic, the EU is elevated to a certain level of importance. Consequently, it gives the EU a more important voice in its own bilateral partnerships. In this

sense, the US – EU partnership is also positional and structural. Both actors promote the protection of human rights off – and online. The use of cyber diplomacy therefore allows the EU to present itself as a serious foreign policy actor and promotes its goals to contribute to a more effective multilateral system. Yet, Günther Oettinger, the former European Commissioner for Digital Affairs, admitted in a speech in 2015 that: 'there are still areas, where we have work to do' (Oettinger 2015).

4.1.4. EU Norm Entrepreneurship

Has the EU had any impact on the norm setting of cyber norms in regard to the US? Following Finnemore and Hollis' definition, norm entrepreneurs have three main strategic tools in order to further norm building: Incentives, persuasion and socialization (Finnemore and Hollis 2016).

As section 4.1.11 illustrated, the understanding of a need for joint norms in cyber is shared by the US and EU. Similarly, the values reflected in such norms are similar to a large extend. The incentives for joint cooperation therefore do not stem form one actor in particular but more from the threat itself. Both the EU and White House recognize that cybercrime in particular lead to large financial losses for consumers and businesses (Finklea and Theohary 2015). From what is accessible in open sources, neither the US nor the EU have actively attempted to incentivize their counterparts. In this regard, the EU cannot be considered as a norm entrepreneur vis-à-vis the US. Cyber security is equally complicated. In this regard, no public utterance or document has outlined incentives by either actor to further invest into cybersecurity, rather the incentive comes from a shared threat perception. Both the US and EU however, incentivize the private sector to further invest into cyber security. The main program for this is the European Commission's initiative 'Digital Single Market' as well as funding research under the Horizon 2020 framework.

Persuasion refers to the basic meaning of the term, urging other actors to take action. In 2012, European Commissioner Malmström called on her American counterparts in a speech to enhance cooperation since 'the bad guys have the upper hand at the moment' (Malmström 2012). However, this statement can rather be seen as reinforcing the need to work together, rather than persuading the US administration to commit to joint action. The need for working together had already been recognized by the US. The fallout from the Snowden scandal and

its implications for data privacy concern in the relations, an important area for cyber criminals, has yet to be evaluated. As noted in 4.1.1., other actors within the European framework have played an important role. The ECJ has struck down the 'safe harbor' agreement on data exchange and as a consequence the two actors have agreed on a new agreement, the Privacy Shield. Commissioner Jourová said in this context: 'the US has assured that it does not conduct mass or indiscriminate surveillance of Europeans. We have established an annual joint review in order to closely monitor the implementation of these commitments.' (European Commission 2016b). Evidently, the verdict and subsequent negotiations enabled the EU to persuade the US to change its data protection approach within the EU. However, to what extend this is only a lip service by the US or whether it has actually changed the behavior remains to be seen.

Norm entrepreneurs make use of social relations to further norms, this process is called socialization. The most important tool of socialization in US-EU relations are joint exercises and establishing 'best practices'. By labelling certain behavior as appropriate and subsequently inappropriate, norms get further pushed towards the norm cascade. As an example, ENISA has published a list with cloud computing certification services which can be trusted (ENISA 2017). Such an act is both incentivizing as it rewards operators and encourages to adhere to certain norms. At the same time, it is socializing, as it leads to set standards which over time will be regarded as the norm. The US and EU share many of such initiatives, and their continuing promotion of the Budapest Convention is the attempt to socialize other states into appropriate behavior.

Concretely, has the partnership with the EU brought any change to the cyber security strategy of the US? The first US cyber strategy has been published in 2003, with the EU lagging behind considerably (Pernik, Wojtkowiak, and Verschoor-Kirss 2016). A broader national security strategy was published in 2010 and updated in 2015, shifting from non-state actor threat focus to state-centered and from political focus to predominantly economic threats linked to cyber (The White House 2015). In 2011, the Obama White House issued the International Strategy for Cyberspace, which puts special emphasis on promoting:

an open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation. To achieve that goal, we will build and

sustain an environment in which norms of responsible behavior guide states' actions, sustain partnerships, and support the rule of law in cyberspace (The White House 2011).

Whilst this approach is also reflected by the EU Cybersecurity strategy, the fact that the US issued their strategy prior to the EU does not indicate that the EU has played a major influence in shaping the US' norm perception towards cyber. None of the statements evaluated by EU officials indicate a use of the three strategies incentives, persuasion and socialization. As outlined, the relationship has had a large effect on European norm construction rather than the other way around. By now, the relationship seems to appear on a level-headed footing with none of the two acting as a single norm entrepreneur towards the other.

4.2 EU – India

4.2.1. Mapping Cyber Relations

Unlike EU-US relations, the dialogue between the EU and India on cyber issues is not nearly as advanced. The base agreement for cooperation, the India-EU strategic Partnership Joint Action plan of 2005, only mentions the issue of cyber once, more specifically the intention to expand the EU-India dialogue in combatting cyber-terrorism. Cooperation on cyber began after a 2010 summit in Brussels, limited to consultations on cyber security and cybercrime. In May 2015, the consultations were elevated to a Cyber Dialogue, within the framework of the bilateral Security Dialogue (Modak et al. 2016). The cyber engagements between India and the EU operate on four different levels: (1) The Cyber Dialogue, which does not address security to a high degree but instead focuses on training programs for India in the field of IT and security, assessment of cybercrime and cooperation on Research and Development, (2) Counter-Terrorism dialogue which focuses on the use of cyber by terrorists, as well as cooperation between the Indian CERT and national and EU CERTs, (3) a Joint Information and Communications Technology Working Group since 2010 with so far 9 meetings, (4) Bilateral security dialogues with EU MS, including France, UK and Germany which also address cyber security issues (Modak et al 2016). The 13th EU-India Summit in Brussels 2016, has advanced the resolve to further deepen and strengthen the EU-India ICT and ICT business dialogue (Council of the European Union 2016b). It is noteworthy however, that a link is drawn between the 'Digital India' initiative and EU's 'Digital Single Market' strategy,

which focuses more on ICT standardization and the economic opportunities of cyber, rather than the cyber security aspect.

Modak et al. identify as a potential dampener for further EU-India cyber relations the Wassenaar Arrangement and the subsequent EU dual-use regime, which all EU countries adhere to (Modak et al. 2016). Dual-use technologies refer to technologies that may be used both offensively and civilian. The Wassenaar Arrangement restricts exports of such technologies of which 'intrusion software', a key element of surveillance systems, is part of (The Wassenaar Arrangement 1996, 72). India specifically has increased widespread mass surveillance since the 2008 Mumbai terror attacks. Whilst this may be an area for further cooperation, it also poses challenges as India is not a member of the arrangement. The arrangement is originally designed to prevent authoritarian states from misusing high-end technology, yet according to Modak et al. India finds itself in a weakened position as it is limited by the agreement, which could have impact on further cooperation. Furthermore, similar to the EU-USA relations, the question of data protection is not addressed adequately within the EU's perception. Accordingly, India does not protect data sufficiently, so that it might be used by cyber criminals. The Indian government however, contests this perception and asserts that it has provided a comprehensive legal framework for privacy and data protection (Modak et al. 2016).

4.2.2. Norm Assessment

Whilst the US and EU share the stance on a multi-stakeholder governance of the internet, with a distribution of power between governments, private actors and civil societies, India's position is somewhat different. The Indian government expresses its reservations towards the multi-stakeholder approach:

> *given the important role that non-government stakeholders play, there should also be a clear delineation of principles governing their participation, including their accountability, representativeness, transparency, and inclusiveness* (NETmundial 2014).

Whilst expressing reservations towards the legitimacy of stakeholders is valid, open and inclusive consultations with such groups have not been conducted by India (Kovacs 2014). According to observers, India would like governments to have the last say in regulating the

participation of non-governmental stakeholders (Kovacs 2014). At this point, there can already be witnessed a schism of norm perception between the EU and Indian approach.

The most contentious issue in EU-Indian relations is the fact, that India has not signed and ratified the Budapest convention. It therefore also is not bound to a defined set of appropriate behaviors, which the charter spells out, such as assisting other countries and sharing information in case of cyber incidents. India feels that the issues of developing countries were not taken into consideration enough, when drafting the convention. The communications minister Kapil Sibal reiterated in 2013 that equity in international cooperation on cyber security was lacking as 'Most of the internet servers are based in the US (and other developed countries) which also decide what kind of information should be on the table for global consumption.' (Singh 2013). This issue casts a shadow over EU-India relations, as the EU has so far struggled to convince its vision of appropriate behavior both in regards to the multi-stakeholder approach as well as the Budapest Convention onto India.

The basis for norms in cyber, or propriety, are to be found in the National Cyber Security Policy, issued by the Indian Department of Electronics and Information in 2013. The cyber security has been criticized for failing to deliver definitions to cyber security, as well as conflating terms and scopes of different forms of cyber security, such as framing fraud and identity theft as a national security issue rather than describing it as cybercrime (Encheva 2016). As a whole the cyber strategy of India, with an overly broad conception of national cyber security, 'risks overwhelming an as yet underdeveloped system with more responsibilities than it may be able to handle' (Encheva 2016).

The EU and India have so far not met collective expectations in regards to cyber norms. As noted above, the fact that the conception of a multi-stakeholder model is challenged by India, albeit it being the world's largest democracy, as well as the non-signature of the Budapest Convention bring difficulties to the cooperation. Yet, common areas such as the Europeans Digital Single Market and the Digital India initiative point to the fact that common denominators have been identified and work on these can further trust in the relations.

4.2.3. Relation Assessment

India is a prime example of the struggle the EU faces in its split between a value driven foreign policy and pragmatism. By establishing a cyber dialogue with India, the EU performs

the ‘positional’ function of partnerships. As such, it has become an interlocutor for global cyber norms by engaging with India. The partnership therefore does not only serve the EU in its bilateral relations with India, but also positions the EU as a global ‘hub’, among others, in global cyber norms relations. As such, the partnership fulfills an integrative function, just as with the US, to contribute to a legitimate European foreign policy. The relational aspect is the most basic form of expectation for a cooperation. Here, the EU and India have identified common objectives in their joint documents, such as strengthening the links between the European Single Market and Digital India. This mainly serves to build trust between the two actors before moving to tackle more contagious issues.

In terms of results, the EU – India partnership has produced limited results if compared to the EU-US cooperation. However, these partnerships are not only results-oriented, but also serve as process-oriented instruments (Renard 2014). As Finnemore and Hollis note, the process of norm entrepreneurship is as important as the final result of the norm cascade (Finnemore and Hollis 2016). Here, the relationship between the EU and India can be interpreted as still being in the process of building common norms, rather than yielding tangible results.

4.2.4. EU Norm Entrepreneurship

The EU is India’s most important trading partner, accounting for 13 percent of India’s overall trade ahead of both China and the US (Pawlak 2016a). However, the degree to which this dependency has been exploited by the EU is rather small. As mentioned in 4.2.1., one of the biggest areas of disagreement remains the question of data security. These have also been part of the India-EU Bilateral Trade and Investment Agreement (BTIA) negotiations, which began in 2007. India has linked the demand for a ‘data secure’ status to these talks, whilst the EU insisted that data protection issues should be separated from the BTIA talks (Menon 2015). It is thus an interesting phenomenon with different angles, the EU does not want to jeopardize trade talks over issues over questions of cyber security and at the same time, it remains strong on these issues in order not to agree to a ‘soft’ deal. Here, the EU could have incentivized India with the BTIA to adopt different data protection rules. Similarly, the EU has offered to assist in the funding of Indian law enforcers. However, India has not yet expressed interest in

pursuing this option. These are just two examples on how the EU is softly incentivizing India to engage in closer cooperation, without yielding results.

The tool of persuasion has so far not been used successfully vis-à-vis India. At the moment, India is still seen as somewhat a 'swing state' in regard to cyber governance. Whilst it prescribes to democratic values and is even aspiring to generate new international laws and treaties on cyber security, as Vinay Kwatra of the Indian Foreign Affairs Office said at a global multi-stakeholder meeting on the future of internet governance (NETmundial 2014), the practice of suppressing civil liberties during times of demonstrations is worrying to the EU (Pawlak 2016b). The lack of persuasion can also be found in the data protection issue, where until now neither the EU nor India have changed their position.

Lastly, despite few tangible results the EU-India Cyber Dialogue points towards a socialization of norms. The ongoing debates and cooperation on cyber issues enhances understanding for the views of both actors. As an example, India specifically disagrees with the Budapest convention as it sees it as 'too western' (Modak et al. 2016). Only through further socialization can the view on cyber norms further converge. The current Cyber Dialogue is the right tool of cyber diplomacy to contribute to this goal.

The cyber security strategy of both India and the EU have been published in 2013. As discussed above, the Indian strategy lacks definitional clarity. Whilst India commits to a democratic internet, it nonetheless sees the government's role stronger than the EU. The value driven approach, as presented by the EU – where specific mention goes towards human rights offline and online – cannot be found in India's strategy. The statements by the Indian government also suggest that it seeks to establish an overarching international treaty in order to tackle internet governance (Kovacs 2014). The EU on the other hand explicitly states that it does not seek to introduce new legislation, but rather wants to strengthen existing multilateral fora (European Commission 2013). Therefore, it can be concluded that the EU has so far not delivered on tangible results but nonetheless has presented itself as an interlocutor on cyber issues.

4.3. EU-Russia

4.3.1. Mapping Cyber Relations

Following the annexation of Crimea by Russia in spring 2014, EU-Russia relations are at an all-time low. This also holds true for cooperation in regards to cyber issues. Relations with Russia are steered by the EU-Russia Information Society Dialogue with the Russian Ministry of Telecoms and Mass Communications. This dialogue includes topics of Russian expertise in ICT, however the progress of these talks is unknown. Before the Ukraine crisis cooperation was more advanced and included measures such as a Russian representative at EC3 to tackle transnational cybercrime more effectively. Russia and the EU also discussed the Russian participation of the Europol initiative 'Check the Web' to combat cyber terrorism as well as exchanging information on harmful viruses used by cybercriminals (Hernandez i Sagrera and Potemkina 2013). In 2009, the Council of the EU instructed Europol to start deepening negotiations for an operational agreement with Russia, however, these negotiations have been suspended following the Ukraine crisis (Renard 2014). In the absence of an agreement, contacts with the Russian Office of the General Prosecutor have nonetheless been established and have yielded success such as a joint seminar (Renard 2014). Indeed, there is no specific EU-Russia forum at the moment in which the two actors meet regularly. Dialogue and cyber diplomacy however continues in different multilateral frameworks such as the UN Group of Governmental Experts (GGE) on cyber security (Bendiek, Berlich, and Metzer 2015). It is in these frameworks that the EU and Russia can work on Confidence Building Measures (CBMs) in order to regain trust – an important component for successful cooperation.

Whilst the Ukraine crisis has brought deterioration to the bilateral relations, cyber relations had already been challenged earlier, in 2007 with the cyberattack on Estonia. Although attribution of cyberattacks to state actors is very complicated, it is widely believed in Western media and governments that Russia was the perpetrator of the attack (Karatzogianni 2010). Since then, the use of cyber as a strategic tool to create turmoil in Western societies has continued, from alleged hacks of the Democratic National Congress in the US elections in 2016 to the release of dozen hacked documents of the – then French presidential candidate – Emmanuel Macron. German security services have also warned that the German elections in fall 2017 could be a target (Herszenhorn 2016).

4.3.2. Norm Assessment

The Russian cyber security strategy was presented in 2000, with a renewal underway. Alike to India and the US, the Russian strategy calls for promoting the establishment of an international legal regime, aimed at creating conditions for the establishment of international information security (CCDCOE 2017). Furthermore, it also makes reference to international organization like the United Nations, G20 and G8 and more specifically regional organizations such as the Shanghai Cooperation, whilst the EU finds no mention in the strategy. The strategy also does not mention the promotion of human rights online, which puts the strategy in stark contrast to the EU and US.

Russia's priority in the cyber strategy states that it aims to 'create conditions for ensuring the technological sovereignty of states in the field of information and communications technologies' (CCDCOE 2017), therefore neglecting the multi-stakeholder approach, promulgated by the EU and US. Whilst other states and actors put high emphasis and competencies with law enforcement to tackle rising cybercrime, the main institution to coordinate cyber policies in Russia is the Foreign Office (CCDCOE 2017). This points to the fact that Russia sees the priority of building cyber norms in international engagement through political means, rather than in closer cooperation of law enforcement agencies.

The Russian strategy makes no specific points on appropriate behavior, however it does recognize that the weak points of the Russian Federation in regards to cyber are insufficient skilled people, a non-competitive scientific and technological potential and an insufficient information industry (Lukasz 2017). If juxtaposed with the newly published National Security Strategy of 2015, it becomes apparent that a strong role is assigned to state sovereignty, also in regards to cyber issues (Oliker 2016). Furthermore, Russia is not a signatory of the Budapest Convention, reflecting its wishes to maintain total sovereignty. Similar to India, Russia considers the information exchange problematic and views it as an infringement of its sovereignty.

Similar to the case of India, the EU and Russia share very few concepts about how norms in cyber security should function. Both of these actors do not recognize the Budapest Convention as an effective legal instrument to tackle cybercrime. Furthermore, open and democratic access to internet with several stakeholders is more of a priority for Western

actors then Russia and India. Russia puts high emphasis on the non-interference of its domestic affairs by foreign actors and sees the concept of sovereignty as paramount in internet governance. Furthermore, the EU and Russia do not trust each other in regards to cyber security. As the EU mentions in it cyber security strategy, it will focus on working with like-minded partner, therefore somewhat including Russia from further international cooperation (Renard 2014).

4.3.3. Relation Assessment

Whilst Russia and the EU have halted bilateral cooperation since the Ukrainian crisis, the two actors nonetheless continue cooperation in multilateral fora such as UN GGE and G20. The EU has also actively supported the establishment of CBM's with Russia in the framework of the OSCE, however not in a bilateral setting. In this sense, the relationship between the EU and Russia is strictly relational. As no specific outcomes are to be expected soon, it is vital to the EU to keep the lines of diplomacy open and remain an interlocutor on cyber issues. However, the process of socialization in this regard will remain a slow one, as tensions keep being high.

4.3.4. EU Norm Entrepreneurship

It lies in the long-term strategic interest of both the EU and Russia to normalize relations in regard to cyber. However, the current political situation makes it highly unlikely that a short-term normalization will occur. As long as Russia is among the regularly accused actors of carrying out cyberattacks, it will be difficult to build a long-term strategy with Russia on how to tackle cyber activities.

Similarly, in terms of persuasion, the EU yields limited leverage over Russia. In international organizations, the EU usually sides with actors such as the US (Renard 2014), creating a front against rogue states such as Russia and China. It has become manifest that two different ways of organizing global internet governance exist, with the EU and Russia on opposing sides. Persuading Russia to put less emphasis on state sovereignty and instead adopt the multi-stakeholder value approach has until now proven impossible for the EU (Renard 2014).

At the very moment, socialization is the only way forward for the two actors to keep open channels and build understanding. Similarly, CBM's can contribute to understanding

each other's different conceptions of norms in cyber security. In this sense, the EU can still act as a norm entrepreneur, however it will be a lengthy process to advance the EU's notion of cyber security. It is difficult to imagine that this will happen in the near future, as long as the political relationship remains as strained as currently.

Finally, as discussed in 4.3.3., the cyber security strategy of Russia and the EU bear little resemblance. The first draft by the Russian Federation had been published prior to the European strategy, with a renewal underway. Assessing the latest renewed national security strategies point to the fact that it will not incorporate the values as promoted by the EU. It is therefore safe to conclude that the EU has not acted as a successful norm entrepreneur vis-à-vis the Russian Federation.

5. Discussion

The case studies have discussed the impact and extend of European bilateral relations in regards to cybercrime and cyber security. In all three cases, not enough evidence could be obtained to support the two main and sub hypotheses. The comparative case study of the US, India and Russia were not able to demonstrate that the EU has decisively acted as a norm entrepreneur in constructing global cyber norms.

Hypothesis 1 attempted to explore whether close working relationships, under the auspice of European cyber diplomacy, may alter the cyber security norms of another state. In case of the US, both actors share to a large extend a similar notion of how cyberspace should be governed. However, it appears as if the US had an effect on the EU rather than vice versa. This largely stems from the fact that the US has been at the forefront of adopting a cyber security strategy, albeit not always very successfully (Stavridis 2017). It can be argued, that the US and EU together act as norm entrepreneurs in promoting a free and open, value based cyber space. This is for example visible in their attempt to jointly promote the Budapest Convention and by creating The Global Alliance against Child Sexual Abuse Online. Yet, as differences are still present, especially in regards to data privacy, cyber espionage and the use of offensive cyber weapons, it cannot be argued that the EU has acted as a norm entrepreneur. This is supported by assessing hypothesis 1a, where similar notions and values for cyber

security can be identified, however, these were present before the EU had formulated their own strategy.

A similar finding can be asserted for EU-India relations. Considering that India is the world's largest democracy with soon nearly 1 billion people having internet access, this partnership is of huge importance to further regulate cyberspace. As the case study finds, India is still a swing state when it comes to cyber security and the role of governments and other actors. The bilateral relationship has great potential and the current approach of focusing on less contested areas such as the 'European Single Digital Market' and 'India Digital' may lead to more success in the future. As of yet, India's cyber security strategy does not reflect the values promulgated by the EU. Similarly, India is not yet a signatory of the Budapest Convention and does not appear to become one anytime soon. In public statements, India is actively calling for the creation of a new legal framework to regulate state behavior in the cyber domain, this is opposed to the EU, which explicitly does not seek new legal frameworks. Thus, although the EU and India have a close working relationship, hypothesis 1 does not find enough support to posit that the EU has acted as a norm entrepreneur in this case.

Russia and the EU have had a strained relationship ever since the annexation of Crimea by the Russian Federation. This is also reflected in the cyber partnerships and cooperation initiatives which have since been put on halt. Unlike the EU, Russia puts great emphasis on the role of state sovereignty in the cyber domain and rejects the multi-stakeholder approach. It cannot be asserted that the EU and Russia have a close working relationship, nor that the values pursued by the EU are reflected in the Russian approach to cyber security. Therefore, hypothesis 1 cannot be supported in the case of Russia.

Considering that in all three cases hypothesis 1 has been rejected, one may also assert that hypothesis 2 must be rejected. Whilst the EU is part of the global debate on how to shape the internet in the future, the tool of cyber diplomacy has not proven futile as of yet. However, norm building may take a long time, considering that the EU has only adapted a cyber security strategy in 2013 these efforts may still be fruitful. Other authors have recognized that the EU has positioned itself as a serious actor and interlocutor of how the internet should be shaped (Renard 2014). This is in line with the European Commission's own position, which seeks to become a 'honest broker' (European Commission 2014a).

The theoretical framework has set out to investigate to what extend the EU is a normative power in regards to cyber security. Ian Manners argued that the EU has by its mere existence contributed to a 'new normal' in international relations (Manners 2002). Indeed, the EU is working with partnerships as a means of cyber diplomacy. Through these partnerships and by positioning itself as a honest broker, even if as of yet, as an unsuccessful norm entrepreneur, the EU has contributed to gain legitimacy in conducting foreign policy. Manners further set four principles which underpin normative power: Ideational, principles, actions and impact (Manners 2009). In the EU's way of conducting cyber diplomacy, these four principles can be found again, albeit impact being the least successful one. However, the actions are grounded in a value driven approach, with principles such as the protection of human rights (online) being anchored in multilateral documents and a cooperation-oriented process, rather than through force or coercion. Sjursen (2006) puts value on the development of cosmopolitan law, where one could argue that the EU through the promotion of the Budapest Convention is attempting to contribute to such. However, the question of how much this is interest driven, or indeed as a 'force for good' remains to be seen.

6. Conclusion

This thesis sought to examine whether the EU can be considered as norm entrepreneur in constructing global norms for cyber security. Considering the debate on the EU as a normative power, a distinct form of power if juxtaposed with other great powers. The debate began in the 1970's as a concept emphasizing on the special civilian position of Europe in between the two great powers USA and USSR. As the debate continued, various authors put their attention on how the EU exerts this normative power, with this debate being taken up and acknowledged by political decision-makers. An important tenant of the debate focuses on the legitimacy of European power, and the legitimacy of European institutions to exert such power. Special attention has been paid to the approach taken by Ian Manners, who differentiates different forms of exercising European normative power and the approach of Sjursen, who sees the legitimacy of normative power by contributing to the formulation of cosmopolitan law.

To conceptualize and operationalize the concept of European normative power further, this thesis paid special attention to norms research in international relation in general, and

the concept of norms entrepreneurs in particular. Norms entrepreneurs follow the norm-life-cycle model, which shows different stages of a norm until it becomes uncontested and thus reaches the norm cascade. The issue of behavior in cyber and constructing norms for appropriate behavior is an especially contested and novel one, as states disagree on what the right way forward is. The EU has pledged itself, through the cyber security strategy of 2013, to promote an open, value-driven, multi-stakeholder model of the internet and to protect the same rights online as offline. In order to further these norms, the EU utilizes cyber diplomacy, essentially traditional diplomacy with regards to the cyber domain, with states that it considers as key partners.

In a comparative case study between the EU and the US, India and Russia, the thesis explored the extend of current cyber relations, how these states view cyber norms and whether the EU has acted as a norm entrepreneur. The hypotheses were that if the EU had close working relationships with these states, it would have an impact on their cyber security strategies and if that would be the case, the EU could be considered a norm entrepreneur. However, in all three cases the two main hypotheses do not seem to be confirmed. Whilst the EU is presenting itself as somewhat of an indispensable interlocutor on cyber issues, it has so far not managed to have a real impact in terms of norm building. However, the EU is acting in a way that relates back to how Manners conceptualized the exert of European normative power.

The study, however, faced severe limitations. As the information gathering was based on desk research, it was difficult to find sound public information on the way the EU is attempting to incentivize and persuade its partners in constructing these norms. Many of the meetings take place behind closed doors, which make access very difficult due to the sensitive nature of the discussed topics. Therefore, the thesis relied largely on secondary information, such as think tank reports and public statements of the actors in question. This makes generalizable statements of the outcomes difficult to verify.

Further research however, could shed light on the interplay of internal and external norm building of the EU in terms of cyber. Recent events have recalled the need for an agreement on how to best tackle the issues that arise from an area which seems underregulated.

Presenting itself as successful in this area could give the EU new legitimacy, especially in regard to its foreign policy ambitions.

7. Abbreviations

BTIA – Bilateral Trade and Investment Agreement

CBM – Confidence Building Measure

CERT – Computer Emergency Response Team

CFSP – Common Foreign and Security Policy

CSDP – Common Defense and Security Policy

DG – Director General

EC3 – European Cybercrime Center

ECJ – European Court of Justice

EDA – European Defense Agency

EEAS – European External Action Service

ENISA – European Agency for Network and Information Security

EU – European Union

GGE – UN Group of Governmental Experts

ICT – Information Communication Technology

ISP – Internet Service Providers

MS – Member States

MSSD – Most Similar System Design

WGCC – Working Group on Cybersecurity and Cybercrime

OSCE – Organization of Security and Cooperation in Europe

8. Bibliography

Aggestam, L. 2008. “Ethical Power Europe?” *Special Issue of International Affairs* 84 (1).

———. 2009. “The World in Our Mind: Normative Power in a Multi-Polar World.” In *Normative Power Europe in a Changing World: A Discussion*, edited by André Gerrits. Vol. Netherlands Institute of International Relations Clingendael. The Hague.

Karatzogianni, A. 2010. “Blame It on the Russians: Tracking the Portrayal of Russians during Cyber Conflict Incidents.” *Digital Icons: Studies in Russian, Eurasian and Central European New Media*, no. 4. https://works.bepress.com/athina_karatzogianni/1/.

Bendiek, A. 2014. “Tests of Partnership: Transatlantic Cooperation in Cyber Security, Internet Governance and Data Protection.” *Stiftung Wissenschaft Und Politik* Research Paper 5.

Bendiek, A., C. Berlich, and T. Metzger. 2015. “The European Union’s Digital Assertiveness.” http://www.ssoar.info/ssoar/handle/document/44591.

Bickerton, C. J. 2011. “Legitimacy through Norms: The Political Limits to Europe’s Normative Power.” In *Normative Power Europe: Empirical and Theoretical Perspectives*, edited by Richard Whitman. New York: Palgrave Macmillan.

Boeke, S. 2016. “First Responder or Last Resort? The Role of the Ministry of Defence in National Cyber Crisis Management in Four European Countries.” https://openaccess.leidenuniv.nl/handle/1887/46615.

Bowen, G. A. 2009. “Document Analysis as a Qualitative Research Method.” *Qualitative Research Journal* 9 (2): 27–40. doi:10.3316/QRJ0902027.

Bush, G. W. 2003. *President George W. Bush: The National Strategy to Secure Cyberspace*. Morgan James Pub.

CCDCOE. 2017. “Basic principles for State Policy of the Russian Federation in the field of International Information Security to 2020.” Accessed May 16. https://ccdcoe.org/sites/default/files/strategy/RU_state-policy.pdf.

CERT-EU. 2013. “CERT-EU Task Force.” European Commission. http://cert.europa.eu/static/RFC2350/RFC2350.pdf.

Checkel, J. L. 2001. “Why Comply? Social Learning and European Identity Change.” *International Organization* 55 (3): 553–88.

Choucri, N., G. Daw Elbait, and S. Madnick. 2012. “What Is Cybersecurity? Explorations in Automated Knowledge Generation.” https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2178616.

Christou, G. 2016. *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy*. UK: Palgrave Macmillan.

Council of Europe. 2014. *Convention on Cybercrime*. *ETS No. 185*.

Council of the European Union. 2008. "A Secure Europe in a Better World: Report on the Implementation of the ESS."

———. 2015. "Council Conclusions on Cyber Diplomacy." 6122/15.

———. 2016a. "Council Conclusions on Countering Hybrid Threats." http://www.consilium.europa.eu/press-releases-pdf/2016/4/164_en.pdf.

———. 2016b. "Joint Statement. 13th EU-India Summit." Brussels.

Crandall, M., and C. Allan. 2015. "Small States and Big Ideas: Estonia's Battle for Cybersecurity Norms." *Contemporary Security Policy* 36 (2): 346–68. doi:10.1080/13523260.2015.1061765.

Danca, D. 2015. "Cyber Diplomacy-A New Component of Foreign Policy." *JL & Admin. Sci.* 3: 91.

Deitelhoff, N., and L. Zimmermann. 2013. "Things We Lost in the Fire: How Different Types of Contestation Affect the Validity of International Norms." *Working Papers* 18. http://mercury.ethz.ch/serviceengine/Files/ISN/175046/ipublicationdocument_singledocument/43e9a5db-ba60-496e-8b92-636350dd61f0/en/PRIF_WP_18.pdf.

Department of Defense. 2015. "The DoD Cyber Strategy." Washington DC: US Department of Defense. https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

Duchêne, F. 1972. "Europe's Role in World Peace." In *Europe Tomorrow*, edited by R. Mayne. London: Fontana.

Encheva, D.. 2016. "India's National Cyber Security Policy in Review." *SCSC Cyber Security Conclave*. http://kenes-exhibitions.com/cybersecurity/blog/indias-national-cyber-security-policy-review/.

Engelkamp, S., K. Glaab, and J. Renner. 2012. "In Der Sprechstunde." *ZIB*, 101–28. doi:10.5771/0946-7165-2012-2-101.

ENISA. 2017. "Cloud Computing Certification - CCSL and CCSM — Resilience and CIIP Portal." https://resilience.enisa.europa.eu/cloud-computing-certification.

European Commission. 2012. “An EU Cybercrime Centre to Fight Online Criminals and Protect E-Consumers.” Press Release. http://europa.eu/rapid/press-release_IP-12-317_en.pdf.

———. 2013. “Joint Communication to the European Parliament, the Council, the European Economic and Social Committee of the Regions: Cybersecurity Strategy of the European Union. An Open, Safe and Secure Cyberspace.” http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=1666.

———. 2014a. “Commission to Pursue Role as Honest Broker in Future Global Negotiations on Internet Governance.” Press Release. Brussels: European Commission. http://europa.eu/rapid/press-release_IP-14-142_en.pdf.

———. 2014b. “Internet Policy and Governance: Europe’s Role in Shaping the Future of Internet Governance.” Communication from the Commission to the European Parliament, the Council. the European Economic and Social Committee and the Committee of the Region.

———. 2016a. “Cybercrime.” Text. *Migration and Home Affairs - European Commission*. https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime_en.

———. 2016b. “EU Commission and United States Agree on New Framework for Transatlantic Data Flows: EU-US Privacy Shield.” Press Release. Strasbourg: European Commission.

“European Commission - PRESS RELEASES - Press Release - Speech: Next Step in the EU - US Cooperation on Cyber Security and Cybercrime.” 2017. Accessed May 9. http://europa.eu/rapid/press-release_SPEECH-13-380_en.htm?locale=en.

European External Action Service. 2014. “Fact Sheet. EU-US Cooperation on Cyber Security and Cyber Space.” http://eeas.europa.eu/archives/docs/statements/docs/2014/140326_01_en.pdf.

Europol. 2017. “European Cybercrime Centre - EC3.” *Europol*. https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3.

Fahey, E. 2014. “The EU’s Cybercrime and Cyber-Security Rulemaking: Mapping the Internal and External Dimensions of EU Security.” *Eur. J. Risk Reg.*, 46.

Finklea, K., and C. Theohary. 2015. “Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement.” Washington DC: Congressional Research Service. https://fas.org/sgp/crs/misc/R42547.pdf.

Finnemore, M., and B. B. Hollis. 2016. “Constructing Norms for Global Cybersecurity.” *American Society of International Law* 110 (3): 4425–79.

Finnemore, M., and K. Sikkink. 1998. “International Norm Dynamics and Political Change.” *International Organization* 52 (4): 887–917.

George, A. L., and A. Bennett. 2004. *Case Studies and Theory Development in the Social Sciences*. Cambridge: MIT Press.

Gerrits, A. 2009. “Normative Power Europe: Introductory Observations on a Controversial Notion.” In *Normative Power Europe in a Changing World: A Discussion*, edited by André Gerrits. Clingendael European Papers 5. The Hague: Clingendael, Netherlands Institute of International Relations. https://www.clingendael.nl/sites/default/files/20091200_cesp_paper_gerrits.pdf.

Helmbrecht, U., S. Purser, and M. Ritter Klejnstrup. 2012. “Cyber Security: Future Challenges and Opportunities.” Heraklion: ENISA.

Herszenhorn, D. M. 2016. “Europe Braces for Russian Hacking in Upcoming Elections.” *POLITICO*. December 13. http://www.politico.eu/article/europe-russia-hacking-elections/.

Hocking, B. L., and J. Melissen. 2015. *Diplomacy in the Digital Age*. Clingendael, Netherlands Institute of International Relations. http://www.egmontinstitute.be/wp-content/uploads/2015/07/DIPLO-IN-DIGITAL-AGE.-PDF.pdf.

House of Lords. 2011. “The EU Internal Security Strategy.” 17th Report of Session 2010-12.

Hsieh, H., and S. E. Shannon. 2005. “Three Approaches to Qualitative Content Analysis.” *Qualitative Health Research* 15.

Kagan, R. 2003. *Of Paradise and Power. America and Europe in the New World Order*. New York: Knopf.

———. 2008. *The Return of Histoy and the End of Dreams*. New York: Alfred A. Knopf.

Katzenstein, P. J., Robert O. Keohane, and Steven D. Krasner. 1998. “International Organization and the Study of World Politics.” *International Organization* 52 (4): 645–85.

Kegel, A. 2016. “US-EU Cybersecurity Relation: Out of the Safe Harbor and Behind the Privacy Shield.” Blog. *The Henry M. Jackson School of International Studies*. https://jsis.washington.edu/news/us-eu-cybersecurity-relations-safe-harbor-behind-privacy-shield/.

Khanna, P. 2008. *The Second World: Empires and Influence in the New Global Order*. New York: Random House.

Kovacs, A. 2014. “Is a Reconciliation of Multistakeholderism and Multilateralism in Internet Governance Possible? India at NETmundial – The Internet Democracy Project.” internet democracy project. https://internetdemocracy.in/reports/india-at-netmundial/.

Krippendorff, K. 1980. *Content Analysis: An Introduction to Its Methodolgy*. London: SAGE Publications.

Loges, B. 2014. “Zwischen Einheit Und Vielfalt.Working Paper.”

Lukasz. 2017. “Interesting Points in New Russian Information Security Doctrine.” *Security, Privacy & Tech Inquiries*. http://blog.lukaszolejnik.com/interesting-points-in-new-russian-information-security-doctrine/.

Malmström, C. 2012. “The European Response to the Rising Cyber Threat.” Washington DC.

Manners, I. 2002. “Normative Power Europe: A Contradiction in Terms?” *Journal of Common Market Studies* 40 (2).

———. 2008. “The Normative Ethics of the European Union.” *Foreign Affairs* 84 (1).

———. 2009. *The EU’s Normative Power in Changing World Politics*. Netherlands Institute of International Relations.

March, J. G., and J. P. Olsen. 1998. “The Institutional Dynamics of International Political Orders.” *International Organization* 52 (4): 943–69.

———. 2006. “The Logic of Appropriateness.” In *The Oxford Handbook of Pubic Policy*. Oxford: Oxford University Press. http://dingo.sbs.arizona.edu/~ggoertz/pol595e/March_Olsen2006.pdf.

Maull, H. W. 1990. “Germany and Japan: The New Civilian Powers.” *Foreign Affairs* 69 (5).

Menon, P. 2015. “India - EU Proposed Free Trade Agreement. Issues Surrounding Data Protection.” NASCOM. http://cis-india.org/a2k/blogs/india-eu-proposed-fta.pdf.

Meulen, N., E. Jo, and S. Soesanto. 2015. “Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses.” Document Requested by the Committee on Civil Liberties, Justice and Home Affairs. Cambridge: European Parliament. http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536470/IPOL_STU(2015)536470_EN.pdf.

Modak, P., K. Kulkarni, A. Phatak, S. Joshi, S. Virkar, A. Rao, and M. Kripalani. 2016. “EU-India Think Tank Twinning Initiative. Moving Forward the EU-India Secuurity Dialogue: Traditional and Emerging Issues.” *Gateway House and Istituto Affari Internazionali*.

NETmundial. 2014. “NETmundial - Welcome Remarks.” Sao Paulo, Brazil. http://netmundial.br/wp-content/uploads/2014/04/NETMundial-23April2014-Welcome-Remarks-en.pdf.

Nye, J. 2002. *The Paradox of American Power*. Oxford: Oxford University Press.

———. 2004. *Soft Power: The Means to Success in World Politics*. Public Affairs. http://faculty.maxwell.syr.edu/rdenever/PPA-730-27/Nye%201990.pdf.

Oettinger, G. 2015. “Speech Cybersecurity Strategy.” May 28.

Oliker, O. 2016. “Unpacking Russia’s New National Security Strategy | Center for Strategic and International Studies.” *Center for Strategic and International Studies*. https://www.csis.org/analysis/unpacking-russias-new-national-security-strategy.

Onuf, N. 1998. “Constructivism: A User’s Manual.” In *International Relations in a Constructed World*. M.E. Sharpe Inc.

OSCE. 2013. “Decision No. 1106 Initial Set of OSCE Confidence-Building Measures to Reduce the Risks of Conflicts Stemming from the Use of Inormation and Communication Technologies.” https://icu.repo.nii.ac.jp/?action=pages_view_main&active_action=repository_view_main_item_detail&item_id=2554&item_no=1&page_id=13&block_id=17.

Pawlak, P. 2016a. “EU-India Cooperation on Cyber Issues: Towards Pragmatic Idealism?” http://www.iai.it/sites/default/files/iaiwp1636.pdf.

———. 2016b. “Resilience in the EU’s Foreign and Security Policy.” Briefing. Brüssel: European Parliament. http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/583828/EPRS_BRI%282016%29583828_EN.pdf.

———. 2017. “Countering Hybrid Threats: EU-NATO Cooperation.” European Parliament. http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/599315/EPRS_BRI(2017)599315_EN.pdf.

Pernik, P., J. Wojtkowiak, and Verschoor-Kirss. 2016. “National Cyber Security Organisation: United States.” Tallin: CCDCOE - Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_USA_122015.pdf.

Renard, T. 2014. “The Rise of Cyber-Diplomacy: The EU, Its Strategic Partners and Cyber-Security.” *ESPO Working Paper* EU Strategic Partnerships and Transnational Threats (7). http://fride.org/descarga/OP_EDC_2020_Subsaharan_Energy_nov09.pdf.

Risse, T. 1999. *The Power of Human Rights. International Norms and Domestic Change*. Cambridge: Cambridge University Press. http://catdir.loc.gov/catdir/samples/cam032/98042345.pdf.

———. 2000. "'Let's Argue!': Communicative Action in World Politics." *International Organization* 54 (1): 1–39. doi:10.1162/002081800551109.

Sagrera, R., and O. Potemkina. 2013. "Russia and the Common Space on Freedom, Security and Justice." *Study for the Directorate General for Internal Policies–Policy Department C: Citizen's Rights and Constitutional Affairs–European Parliament*. https://www.ceps.eu/system/files/No%2054%20EP%20Study%20-%20EU-Russia%20Comman%20Space%20on%20Freedom%20Security%20and%20Justice.pdf.

Shalini, S. 2016. "Budapest Convention on Cybercrime." Information Law and Policy Research at the Centre for Communication Governance. *The CCG Blog*. https://ccgnludelhi.wordpress.com/2016/03/03/budapest-convention-on-cybercrime-an-overview/.

Singh, P. 2013. "India Won't Sign Budapest Pact on Cyber Security." *Governance Now*. http://www.governancenow.com/news/regular-story/india-wont-sign-budapest-pact-cyber-security.

Sjursen, H. 2006. "The EU as a 'Normative' Power: How Can This Be?" *Journal of European Public Policy* 13 (2): 235–51. doi:10.1080/13501760500451667.

Sliwinski, K. 2014. "Moving beyond the European Union's Weakness as a Cyber-Security Agent." *Contemporary Security Policy* 35 (3): 468–86. doi:10.1080/13523260.2014.959261.

Smith, H. 2002. *European Union Foreign Policy: What It Is and What It Does.* London: Pluto Press.

Smith, K. E. 2000. "The End of Civilian Rower EU: A Welcome Demise or Cause for Corncern?" *The International Spectator* 35 (2): 11–28.

Smith, M.H., S. Keukeleire, and S. Vanhoonacker. 2016. "Introduction." In *The Diplomatic System of the European Union: Evolution, Change and Challenges*, edited by M.H. Smith, S. Keukeleire, and S. Vanhoonacker. Abingdon: Routledge.

Solms, R. and J. Niekerk. 2013. "From Information Security to Cyber Security." *Computers & Security* 38 (October): 97–102. doi:10.1016/j.cose.2013.04.004.

Telò, M. 2007. *Europe: A Civilian Power? European Union, Global Governance, World Order*. Basingstoke and New York: Macmillan.

The Wassenaar Arrangement. 1996. *List of Dual-Use Goods and Technologies and Munitions*.

The White House. 2011. “International Strategy for Cyberspace.” Washington DC: The White House. https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

———. 2015. “National Security Strategy.” Washington DC: White House. https://ccdcoe.org/sites/default/files/strategy/USA_NSS2015.pdf.

Tirrmaa-Klaar, H. 2013. “Cyber Diplomacy: Agenda, Challenges and Mission.” In *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy*, edited by Katharina Ziolkowski. Tallinn: NATO CCD COE Publication.

“Viewpoints: Cyber Security and Cyber Defence in the European Union.” 2017. Accessed March 23. https://www.eda.europa.eu/info-hub/opinion/2014/06/11/viewpoints-cyber-security-and-cyber-defence-in-the-european-union.

Warner, M. 2012. “Cybersecurity: A Pre-History.” *Intelligence and National Security* 27 (5): 781–99. doi:10.1080/02684527.2012.708530.

Wiener, A. 2014. *A Theory of Contestation*. Heidelberg: Springer.

Wiener, A., and U. Puetter. 2009. “Quality of Norms Is What Actors Make of It Critical-Constructivist Research on Norms, The.” *J. Int’l L & Int’l Rel.* 5: 1.