Lund University
Department of Political Science

STVM23
Supervisor: Ian Manners

Cyber Normativity

A Qualitative Case Study Explaining the European Union's Normative Power in the 2020 Cybersecurity Strategy

LUND UNIVERSITY

Frida Moisiola

Master of Science in European Affairs

Spring of 2024

Abstract

The European Union has developed a critical concern for cybersecurity, requiring a comprehensive approach to tackle new challenges arising from cyber threats. Against the backdrop of increasing global cyber-attacks and emerging regulatory models from rival powers, such as China and Russia, the EU has positioned itself as a key player in cybersecurity policy. This thesis researches the extent to which the European Union acts as a normative power within cybersecurity. The essay uses qualitative content analysis based on the EU's 2020 Cyber Security Strategy and Normative Power Europe (NPE) to shed light on how the EU operationalizes its normative aspirations in cybersecurity. The analysis ascertains whether other perspectives on European power, such as Market Power Europe (MPE), have better explanatory power. This thesis argues that while the EU exhibits normative intent in cybersecurity, it also pursues market-oriented self-interests, aligning with the MPE framework. While the EU generally meets the criteria for normative power, occasional shortcomings in balancing normative intent with self-interest and inclusiveness in normative processes are evident. Limitations of detecting normative impact further underscore the need for more comprehensive studies. Furthermore, investigating the intersection of cybersecurity and military strategy is a compelling topic for future inquiry.

Key words: European Union, Cybersecurity, Cybersecurity Strategy, Normative Power, Capacity Building
Words: 19863

Table of Abbreviations

CCB	Cyber Capacity Building
CPE	Civilian Power Europe
EC	European Commission
ENISA	The European Union Agency for Cybersecurity
EU	European Union
EUCSS	European Union’s 2020 Cyber Security Strategy
MPE	Market Power Europe
NPE	Normative Power Europe

Table of contents

1. Introduction: Cybersecurity as a Growing Challenge for the European Union

Cybersecurity has moved from being a national concern to a global challenge with cyber threats now transcending borders and becoming a significant challenge to nations and organisations alike. As cyber-attacks are becoming more frequent and sophisticated, there has been a growing need for the EU to act. The EU has therefore positioned itself as a key actor by developing a comprehensive approach to cybersecurity through its various cybersecurity strategies. A new cyber security strategy was presented by the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy at the end of 2020 (EC 2020b). This strategy includes updates of existing initiatives as well as new directives, with the overarching purpose of strengthening the EU's resilience to cyber threats. The EU's commitment to addressing cybersecurity is a central part of its overall strategy for the digital transformation of society to ensure digital safety for all EU citizens. As expressed by the EU, the new cybersecurity strategy also enables the EU to take on a leading role in cybersecurity regarding international norms and standards. This includes the promotion of a global, open, stable, and secure cyberspace (EC 2020a). Examining the EU's cybersecurity approach is necessary in order to understand how the EU navigates a complex digital landscape and tackles these new challenges.

A key issue in this regard is who should lead the effort to govern and regulate the internet and cyberspace. There is global competition over this digital landscape and the nature of the rules where the EU is not the only exporter of cybersecurity policies. Alternative models have emerged, often in opposition to the EU's ambitions, notably from China and Russia. These contain elements that risk threatening the fundamental freedoms, human rights, and democracy that the EU stands for (Anagnostakis 2022, Renard 2018).

As part of the EU's strategy, the EU has therefore been actively engaged in so-called strategic partnerships with various third parties. These external engagements are part of the EU's efforts to strengthen international cooperation and address common challenges in the field of cybersecurity. The EU typically engages in cyber dialogues with like-minded partners and other international actors to promote secure cyberspace abroad. These dialogues cover a variety of topics, such as cybersecurity norms, capacity building, and the development of international rules and standards in cyberspace (Anagnostakis 2022, EC 2024). The EU is actively involved in assisting third countries, such as those in the Western Balkans and the Eastern Partnership countries, in enhancing their capacity to defend themselves against cybersecurity threats (Cybil 2024b). Recently, there have been increasing divisions among Member States on whether cybersecurity should be regulated, and which actors should be involved. In some cases, disagreements have arisen where some Member States want to prioritise pure security over rights in their national strategies. This contradiction creates incoherence internally which ultimately threatens the EU's ability to be a major power in the global arena (Pâris 2021).

1.1 Purpose and Research Question

Given this currently evolving field, the challenges facing the EU and the normative ambitions expressed by the EU (EC 2020a), it becomes essential to understand the EU's normative role in cybersecurity in more depth. While existing research has extensively examined the EU as a normative power from various angles, there remains a notable gap in understanding its actions and influence in the cybersecurity domain, particularly in relation to third countries.

The purpose of this thesis is therefore to investigate the extent to which the EU acts as a normative power in cybersecurity and its implications for relations with third countries. This is conducted by employing the lens of Normative Power Europe (NPE) developed by Ian Manners. NPE theory establishes that the EU seeks to promote its principles and values to shape international norms and behaviour (Manners 2002). In the context of cybersecurity, this would entail the establishing of standards aligned with EU values to influence global cybersecurity norms. By examining the EU's latest cybersecurity strategy from 2020, consisting of policies, projects and cooperation efforts, this study aims to shed

light on how the EU operationalizes its normative aspirations in the cybersecurity realm and its impact on global cybersecurity governance. The aim is also to test whether NPE can explain the EU's behaviour or whether other perspectives on European power, such as Market Power Europe (MPE) offer better explanations. This research aims to address the current research gap by providing a comprehensive analysis of the current EU cybersecurity strategy in relation to its normative objectives. By examining the EU's actions and external engagement in cybersecurity, the study aims to contribute to the debate on digital governance and the EU's role in shaping the global cybersecurity agenda. Moreover, this research challenges notions of security and power that the EU traditionally has been linked to. European power has traditionally been associated with military capabilities. However, in an era where digitalisation plays an increasing role in our lives, cybersecurity emerges as a critical domain where normative power plays a central role alongside traditional forms of power. This research aims to provide insights into the dynamics of this interplay. Building upon the problem formulation and purpose outlined above, the research question is as follows: **To what extent does the European Union act as a normative power within cybersecurity?** This question allows for an examination of the EU's normative ambitions in its relations with third countries and its broader impact on international cybersecurity. By assessing the extent to which the EU embodies normative power in cybersecurity, this question focuses on the EU's ability to shape global cybersecurity norms and behaviours. This research question thus makes it possible to capture the essence of the study's purpose, which is to clarify the EU's normativity in the field of cybersecurity.

The following chapter lays out the current research field on the EU and its cybersecurity challenges as well as its normativity. Chapter three covers a discussion of theoretical perspectives on European power and presents the theoretical approach for this thesis. Chapter Four sets out the design and method used for conducting the empirical study. Next follows an analysis of the findings and their theoretical implications. Thereafter follows a conclusion that establishes that the EU’s approach to cybersecurity reflects both normative aspirations and its role as a market power as the EU is shaping cyber norms through a combination of value promotion and market-oriented self-interest. Lastly is a brief reflection on lessons learned through the research process as well as topics for further research.

2. Previous research: Unravelling the European Union's Cybersecurity Challenges

EU and cybersecurity are multifaceted research fields where researchers take on various approaches. In terms of the EU's influence and power over this process, certain research focus can be discerned in previous research. Many researchers study questions about the kind of actor the EU is within cybersecurity and the challenges that the EU faces in being a major leader in the field. Among these challenges have coherence, competing norms with other countries, and too many involved actors stood out as the most significant. Another strand of research looks more closely at the effectiveness of the EU's external initiatives and discusses the initiatives in terms of how successful they have been, although not necessarily from a normative perspective. My research builds on these discourses but differs in terms of the focus. Previous research is, however, very valuable in gaining the necessary insights into what can explain the EU's actions. There is widespread research on the EU as a normative power, which will be laid out in Chapter Three. However, there is limited research on the EU as a normative power in the context of cybersecurity. This research gap is what this thesis hopes to fill.

2.1 EU as an Actor in Cybersecurity

When compared to other major cybersecurity players, the EU's actorness in cyberspace is still rather limited (Carrapico & Barrinha 2017). Even though the EU has a stated ambition to be a coherent cybersecurity actor there are several factors that limit this intent (ibid). As previously mentioned, a recurring challenge to the EU's cybersecurity strategy is the current diversions among member states, as well as fragmentation in cooperation between the different actors involved. Both Carrapico & Barrinha (2017:1256) and Pâris (2021:14) divide coherence into two categories: institutional cooperation and a common understanding of security. Institutional cooperation places great rhetorical emphasis on the development of a common approach to cybersecurity based on increased cooperation between actors, instruments, and policies (Carrapico & Barrinha 2017:1257, Pâris 2021:15) Such cooperation is particularly important given that the EU's approach to cybersecurity is decentralised with bodies involved from both the private and public sectors. Coherence as a common understanding of security is directly linked to the perceived need for an EU cybersecurity strategy (Carrapico & Barrinha 2017:1258).

Diverging interests and priorities in the Member States contribute to the disintegration of cybersecurity. The EU faces challenges in establishing a shared vision for cybersecurity due to its intergovernmental structure. This issue stems from a fundamental lack of consensus within the EU regarding the comprehensive understanding of cyber security (Sliwinski 2014). Pâris argues that hesitant Member States remain a challenge to the EU's coherence in the field (Pâris 2021:1). One reason is that there is internal division as Member States (via the Council) tend to be more reluctant than other institutions (such as the EP) to surrender power to the EU in this area (Carrapico & Barrinha 2017:1264). Considering that cyber issues are tied to sovereignty, certain member states harbour scepticism regarding EU intervention and a shared perspective on cybersecurity. An example of this can be found in the implementation of the NIS directive. Although all Member States approved of the directive, certain Member States hesitated to confer upon the EU increased authority in overseeing their cyber activities (Pâris 2021:16-17). It is also possible to identify several differences among Member States. For instance, countries like France, Germany, and the Netherlands advocate for measures beyond those outlined in the EU cybersecurity framework, whereas other countries have opted for forms of sub-regional cooperation. An example of such sub-regional cooperation is the V4 countries together with Austria that created the Central European Cyber Security Platform (CSCSP) (Carrapico & Barrinha 2017:1264-1265). Furthermore, not every Member State prioritises cybersecurity at the level that the EU does and is therefore not as willing to make the financial commitments required to create the infrastructure to pursue the EU's security ambitions (Carrapico & Barrinha 2017). Given this, the EU consists of countries both highly committed to meeting cybersecurity requirements and others being less advanced (Pâris 2021:18, Kasper 2020)

Pâris (2021) argues that the EU undoubtedly holds a significant position as a regional cyber power. As the EU seeks to establish itself as a formidable global diplomatic entity, it aspires to enhance its international role as a cyber player capable of addressing crises, advocating for its vision, disseminating its values and norms, and safeguarding its interests along with those of its partners. The initiation of a proactive role of the EU in international cyberspace policymaking began with the endorsement of European Council conclusions on cyber-diplomacy in 2015 (Pâris 2021:18). Its primary objective was to advance the establishment of "a global, open, free, stable and secure cyberspace where

human rights and fundamental freedoms and the rule of law fully apply" (Council of the European Union 2019:2). In pursuit of this goal to evolve into an international diplomatic and security actor, the EU aimed to forge robust multilateral and bilateral networks, strengthen strategic partnerships with fellow cyber players, and enhance the cyber resilience and capacities of third countries (Pâris 2021:18). This is part of what this thesis will investigate further. The research aims to find out how normative power influences the EU's external engagements in the cyber security strategy, which in its extension hopes to reveal something about what kind of power the EU has in cybersecurity. The research field on coherence is, therefore, necessary to know the basis for EU action within the field and contribute to conclusions when analysing the findings. It is also important to have mapped the research field, including coherence, to derive the research gap that this thesis wishes to fill.

2.2 Global Competition

Increasingly, other countries have emerged as powers wanting to govern and regulate the norms of the cybersecurity landscape (Anagnostakis 2022). Major challenges to the EU's overarching cybersecurity and digital agenda have persistently emanated from key cyber powers, with notable players including Russia and China (Anagnostakis 2022, Renard 2018). It has become clear that the EU is no longer the only exporter of cybersecurity strategies, where alternative models often contradict the core norms the EU wishes to promote (Anagnostakis 2022:244). One of the most important tools that the EU promotes is the Budapest Convention (Council of Europe 2001). Russia and China on the other hand support the negotiations for a new and different treaty that threatens the fundamental freedoms, human rights, and democracy associated with the Budapest Convention and the EU (Anagnostakis 2022:247, Pawlak 2016). Several international players have significant resources to formulate cyberspace policies and capabilities domestically and in external nations, aiming to fulfil national security goals and influence the establishment of regulations in the field (Pawlak 2016:83). These challengers come mainly from the BRICS countries (Pawlak 2016:85).

Anagnostakis argues that three core elements in the EU's model for good cyber governance are especially contested globally. The first is the Budapest Convention on Cybercrime, the second is the multistakeholder model of Internet governance, and the third is the application of human rights and fundamental freedoms online (Anagnostakis 2022:239-240). For example, both Russia and China insist that states should be able to have increased control of the regulations regarding Internet governance (Wood et al, 2020). Russia and China perceive the heightened participation of the private sector and civil society in current internet governance and mechanisms as unwarranted foreign interference and thus a breach of cyber-state sovereignty (Anagnostakis 2022:245).

These developments have proven to have consequences not only internationally, but also bilaterally (Anagnostakis 2022:248), challenging the EU's efforts with cyber-capacity building (CCB). On a bilateral scale, the EU has initiated CCB programs with neighbouring countries, urging them to adopt and adapt EU models and regulations within their national context (Anagnostakis 2022:253). In contrast to the international arena where the EU employs softer mechanisms like persuasion, argumentation, and socialization, at the bilateral level, the EU offers financial support and technical expertise in return for reforms aligning domestic legislation with EU standards and rules (ibid). China's 'Belt and Road Initiative' is an example of a counterpart to this initiative. This initiative involves financing for the construction and expansion of a nation's digital infrastructure, and proposals for legislative reforms related to cybersecurity that mirror China's laws, often including internet censorship rules, restriction of freedom, and more surveillance (Anagnostakis 2022:249). Partnering with China on these issues can be appealing for authoritarian states as they get the same benefits as from the EU but with the privilege of not having to implement any new legislation for the protection of human rights and freedoms in return. According to Haroche (2022), recent EU development finance projects have been designed in response to the Belt and Road Initiative. These tendencies are further visible in the case of India which initiated cyber dialogues with the EU in 2015. However, India has still not joined the Budapest Convention and instead recently supported Russia's initiative for a new treaty (Anagnostakis 2022:246). Latin America and Africa are leaning towards China and Russia's versions of cyber policy. This has been evident through studying several countries' voting patterns in the UN (Izycki et al 2023). This stresses the importance of the EU to further their engagement in

a values-based approach, including capacity-building and information sharing, with the third countries.

The debate about the EU in competition with other countries' cybersecurity strategies becomes symbolic of the competition between the EU's norms versus the norms of opposing actors. It further stresses the need for and importance of the EU to actively promote its norms and values to be able to govern the field in the way considered rightful. As I conduct this research with NPE as a starting point, the ethical considerations currently challenged by competing actors will probably be apparent in the empirical material.

2.3 EU's External Cyber Engagements

The idea to enhance the European Union's cybersecurity and CCB initiatives abroad was initially emphasised in the 2013 EU Cybersecurity Strategy (EC 2013). After the global malware attacks during the spring of 2017, the Estonian Presidency of the Council of the EU, along with the European Commission and the European Parliament, reached an agreement later that year (EC 2017). This communication advocated for the establishment of the EU Cyber Capacity Building Network (EU CyberNet 2024), designed to bolster the ongoing and forthcoming CCB endeavours of the EU in third countries (ibid). Through CCB, the EU has the authority to determine the approach for enhancing the region's capabilities in utilising cyberspace through collaborative agreements, partnerships, or cooperative arrangements (Bendiek 2018:6). EU recognizes the significance of enhancing capacities in third countries as an element in advancing and safeguarding human rights, the Rule of Law, security, growth, and development (Council of the European Union 2015:9). According to some, capacity building may be used to pursue other objectives rather than purely developmental benefits for the third country to advance national interests and norms. The EU and similar-minded nations have prioritised the safeguarding of their fundamental values, such as democratic principles, human rights, and the rule of law, as well as their strategic interests, forming the foundation of their approach to cyber diplomacy initiatives (Pawlak 2016).

Following their shift from focusing solely on cybercrime to adopting a more comprehensive approach encompassing security and defence, external CCB initiatives have sought to reshape the EU's global security landscape in alignment with the values and strategic interests outlined by Brussels. The significance of external CCB is paramount for the EU's cyber diplomatic endeavours, playing a crucial role in enhancing the EU's strategic collaboration with both its Eastern and Southern neighbourhoods (Carver 2023:13). The aim of this paper is not to focus on the technicalities of capacity building programs. However, to maintain accuracy throughout the paper it is necessary to establish what definition is used in this research. According to the 2018 Operational Guidance for the EU International Cooperation on Cyber Capacity, “capacity building in the cyber domain aims to build functioning and accountable institutions to respond effectively to cybercrime and to strengthen a country's cyber resilience” (EU CyberNet 2018:10). It is this interpretation of capacity building that is used hereafter. EU has furthermore initiated cyber dialogues with several key partners. Usually, these are biannual and annual meetings between EU officials and representatives of third countries (Anagnostakis 2022). For example, the EU conducts bilateral cyber dialogues under its strategic partnership agreements with countries such as the USA, Canada, China, and South Korea among others (Bendiek 2018:5). The 2017 Cyber Security Strategy emphasises the need for the EU to “step up dialogues with third countries to promote global convergence and responsible behaviour in this area” (EC 2017:19). The dialogues have developed with the aim of influencing the behaviour and attitude of its dialogue partners (Bendiek 2018:6).

2.4 EU’s Normative Power within Cybersecurity

As stated in the research purpose there is a lack of research combining the EU as a normative power with the field of cybersecurity. However, an author who indeed studied this is Kondrotas (2021) who poses the question of what effect EU policy has at the international level. He examines this by looking at whether the EU can act as a normative power in cybersecurity, mainly through sanctions as a tool stemming from the Cyber Diplomacy Toolbox. This is to answer the question of whether the EU can become a leader in cybersecurity.

Just like other authors (Anagnostakis 2022, Renard 2018, Pawlak 2016), Kondrotas highlights the struggle between the EU and the other major players in the field; the US, Russia, and China, and how their national cybersecurity strategies differ from the EU and its normative ambitions. China's approach has clear links to the Chinese government and is characterised by a high level of restriction and control of information. This is particularly worrying given the expansion of China's Belt and Road Initiative to third countries. Against this background, he notes the limitations that the EU faces in imposing its views and regulations on other states, particularly regarding cybersecurity. Unlike certain areas where the EU has been able to exert influence over weaker European states, the EU cannot unilaterally pressure other countries to accept its norms and regulations in the cyber domain. The EU lacks the power to impose its internal norms as international standards, and international norms are typically established through interactions among various international actors, primarily states. Therefore, establishing norms in the cyber domain will require collaboration and negotiation among these actors rather than unilateral imposition by the EU. For the EU to ensure that its norms and values become part of the 'normal', it must put itself in a position to convince the other powers of the benefits of these values and the need for such a rules-based cyber regime. Looking at the effectiveness of the sanctions in the EU-US case, Kondrotas notes that the sanctions have had no meaningful effect on the US. This is because the US already had a similar policy to the EU and took similar measures in the field of cybersecurity. The norms of both actors are moving in the same direction and the US and the EU can be seen as being on the same page in terms of cybersecurity norms. EU ideas on cybersecurity governance have failed to influence China's approach, probably because the norms underpinning the EU's vision conflict too much with China's interests. Cybersecurity sanctions against

Russia have also had no limiting or coercive effects, meaning that they have not been able to reinforce the EU's efforts to change Russia's behaviour.

Kondrotas' research is relevant to this thesis as it addresses similar questions to the ones this research aims to answer. However, he focuses on sanctions as an EU tool for norm diffusion, which this research is not limited to. He opens for interesting conclusions on how the EU has difficulty imposing normative effects on states that stand far from them normatively. It remains to be seen whether this will be discernible in this study. Just like Kondrotas' research, this thesis uses the normative framework of NPE. By doing this, the research will hopefully further develop the ideas presented in Kondrotas' research and add insights more directly connected to the research question of this paper. The theoretical framework plays a big part in this process and is thus laid out in the next chapter on theory.

3. Theory: Unpacking European Power - Traditional Perspectives, Normative Power, and Market Power Europe

3.1 Traditional perspectives on European power

The nature of the EU's power has long been a hotly debated topic among scholars, and several concepts and terms have been used to describe the EU's international identity. The three most prominent are Civilian Power Europe (CPE), Military Power Europe, and Normative Power Europe (NPE). The growing discussion surrounding the EU's global identity reflects not just its expanding impact, but also its newfound position as a player in international security following the Cold War era (Kim & Choi 2020).

In 1972, François Duchêne defined the EU as civilian by saying that the EU is a special international actor whose strength lies in its ability to promote and encourage stability through economic and political means (Duchêne 1972). Duchêne's concept of CPE underscores the EU's commitment to global responsibility. The EU's international engagement focuses on addressing longstanding conflicts and violence through non-military methods such as diplomacy, dialogue, and negotiation (Duchêne 1972:43).

Duchêne's idea highlights aspects such as low politics, non-state actors, ideational influences, and international interdependence (Orbie, 2006:124). EU does not rely on military capabilities and strengths, but rather uses its growing economic strength to exercise influence internationally as "economic interests are in the driving seat" (Duchêne, 1994:388). Therefore, tools such as trade and conditionality are important capabilities (Sjursen 2006a:238). Similarly, Twitchett (1976) and Maull (1990) argue that CPE places trust in diplomacy and dialogue, favouring them over military coercion to address international issues. In general, civilian power can be defined by three key aspects: diplomatic collaboration for addressing global issues, emphasis on economic influence to achieve national goals, and the presence of legally binding supranational institutions (Manners 2002).

Bull (1982) later criticised the notion of CPE and argued for Military Power Europe as an alternative concept. His main argument was that Duchêne's idea of civilian power was insufficient and ineffective as regards military capabilities, and thus saw the need to turn the European Community into a military power. The main argument of Military Power Europe is that the establishment of the Common Security and Defence Policy aimed to mirror the EU's strategic vision of providing efficient, coherent, and uniform responses to regional, interregional, and global conflicts and crises. Despite Bull's criticism, CPE and Military Power Europe share several common assumptions. Among these are the perceived immutability of the nation-state, the significance of direct physical strength, and the concept of national interests (Manners 2002). While civilian power focuses on the limited use of physical force and military power, it inherently recognizes the significance of material power (Whitman 2011:4), even though such material would be of economic character (Manners 2002).

3.2 Normative Power Europe by Ian Manners

What kind of power the EU possesses is a continually debated issue. This section will lay out the premises for NPE as introduced by Ian Manners in 2002. In its essence, Manners challenges the traditional perceptions of European power and proposes the alternative of normative power. Doing so, he objects to the conception of the EU being either a military or civilian power and disregards the importance of capabilities. NPE is a contribution to how we better can understand the EU's international role by focusing on ideational rather than military and/or civilian notions of power. Thus, Manners derives the basis of NPE from the phenomena of power over opinion (Carr 1962) as well as power over ideas (Galtung 1973). By adhering to that way of thinking one can begin understanding the EU's international identity. The idea emerged as a reaction to the lack of theoretical discussions on norms and with the intention of moving away from the Cold War-era division between civil and military power (Whitman 2011). NPE views the international community as comprised of diverse actors and opposes the tendency to confine international activities solely to interactions between states (ibid). EU's foundation rests largely on its norms and values that the EU also wishes to promote on the international scene. The following is stated in the Treaty of the European Union: "The Union's action on the international scene shall be guided by the principles which have inspired its own creation, development, and enlargement, and which it seeks to advance in the wider world: democracy, the rule of law, the universality and indivisibility of human rights and fundamental freedoms, respect for human dignity, the principles of equality and solidarity, and respect for the principles of the United Nations Charter and international law" (TEU 2012 Article 21). However, even earlier in the 1973 Copenhagen Declaration on European identity were these values laid out for the first time. EU's foreign and development policy continues to be informed by these norms and values.

Manners (2002) identifies five core norms and four minor norms. Peace and liberty have historical origins and can be traced back to the post-war period. Democracy, Rule of Law and human rights are fundamental freedoms that came to have increasing importance in the effort to distinguish western Europe from communist eastern Europe. Additionally, the minor norms consist of social solidarity, anti-discrimination, sustainable development, and good governance. Acknowledging the EU's normative basis, the question remains how the EU can spread these norms. Manners offers six factors to how

this is done. Contagion happens when norms are diffused unintentionally from the EU to other political actors by leading by example in regional integration. Informational diffusion arises from various strategic communication efforts, including the introduction of new policy initiatives by the EU and declaratory communications. These can for example manifest as initiatives put forth by the EU presidency or the President of the Commission. Procedural diffusion entails the establishment of a formalised relationship between the EU and an external entity. This could take the form of an inter-regional cooperation agreement, participation in an international organisation, or the expansion of the EU through enlargement processes. Diffusion through transference occurs when the EU engages in the exchange of goods, trade, aid, or technical assistance with external parties, primarily through substantive or financial mechanisms. This transfer of resources and support may stem from the exportation of community norms and standards by the EU. The procedural diffusion and diffusion by transference are both accompanied by conditionality which is frequently used by the EU in partner agreements. Overt diffusion refers to the spreading of norms caused by the physical presence of the EU in third countries. This can for example be in the form of Member State embassies. Lastly, cultural filter influences the reception and impact of international norms and political learning in third states and organisations, determining whether these entities embrace, adapt to, or reject these norms. The EU, lacking the conventional tools of 'hard power' like military and cyber capabilities due to its non-state status, is gradually developing a cyber defence policy. However, akin to its approach in various other policy domains, the EU seeks to establish its presence on the global stage by leveraging 'soft power' assets and diplomatic expertise (Renard 2018:326). Normative power and soft power are, to some extent, linked in the sense that coercion would negatively influence the perceived ‘legitimacy’ of EU policies and actions (on which NPE to a considerable degree depends) (Niemann & de Wekker 2010).

Although it is possible to make some comparisons with CPE and NPE, there are certain aspects that differentiate them. It is true that Manners’ NPE sometimes is mixed up with Duchêne’s CPE, as both focus on the importance of non-military power within European states above military means (Whitman 2011:4). And according to Diez (2005) the two might be seen as part of the same discourse that positions the EU as a positive force in international politics. This makes sense considering Duchêne’s argument that Europe” must be a force for the international diffusion of civilian and democratic standards” and

promote values such as" equality, justice, and tolerance" (Duchêne 1973:20). However, even though Manners acknowledges the normative aspect in CPE, he asserts that the capacity to employ civilian instruments constitutes the primary feature of a CPE. Hence, he introduced NPE, suggesting the capability to influence perceptions of what is considered normal in international relations (Orbie 2006). NPE stands apart from debates about soft versus hard power or CPE versus Military Power Europe. The concept emerged in response to a lack of normative theorizing and aimed to transcend the Cold War-era dichotomies of civil versus military power (Whitman 2011:4). Manners' conviction was that conventional understandings of the EU as a civilian power overlooked the advancing of democratic principles globally as its objectives. NPE would thus be a way to move away from these conventional perceptions of the EU as a state-like entity (Whitman 2011:84). Essentially, this means that CPE and NPE differ in both its objectives and its means.

3.3 Criticism

Since Manners' influential publication in 2002, NPE has been a hotly debated issue on several accounts. Jenichen (2022) develops Manners´ ideas of NPE as she suggests the need to make NPE more flexible and nuanced. In her attempt to do this, she investigates norm selection where she tries to find out why the EU chooses to promote some norms and some not, focusing on norms that are internally contested. Furthermore, NPE has faced considerable criticism, particularly from scholars with a structural-realist or rationalist perspective. According to this viewpoint, the EU isn't seen as a distinct actor separate from its member states. Instead, it's believed that influential member states use the EU as a tool to collectively exert hegemonic power, shaping neighbouring regions to align with their own strategic and economic interests (Hyde-Price 2006: 226–7).

Scholars have also criticised that the EU tends to promote an "our size fits all" approach (Bicchi 2006) and that the EU seeks to maximise its own interests regardless of the interests of others (Youngs 2004). Bicchi (2006) underscores the importance of the EU being flexible and having the capacity to adapt policies based on the specific needs of the recipient revealed by the effect of the policies on the targeted areas, so-called reflexivity. Diez and Pace (2007:13) go further in arguing how the EU on its own cannot shape

conceptions of what is considered normal, but that this depends on whether other actors accept the role that the EU wish to project internationally. They argue that NPE is first and foremost a discourse in which EU actors themselves construct themselves as "model citizens" (Diez and Pace 2007:2). According to this logic, the EU will only be a positive force of power to the extent that others can accept it (ibid:13). Neglecting the perspectives and assessments of the parties receiving the EU's actions thus jeopardises the EU's credibility and any conclusions about the EU as a normative power cannot be drawn without assessing the reactions "on the ground" (Noutcheva 2009:1066). Noutcheva (2009:1074) suggests that if a foreign policy is genuinely normative, domestic players affected by it will accept and voluntarily adhere to the normative pressures for change. When a foreign policy actor possesses normative power, it will encounter no resistance to its calls for behavioural change. Even without a universal normative agenda, an action may be deemed normatively legitimate if domestic actors perceive the expected behaviour as normal and do not contest external pressure for adaptation. This dynamic has raised concerns about a potential Eurocentrism and soft imperialism approach (Hettne & Söderbaum 2005). Manners suggests that the impact of actions should be assessed, with a focus on minimising harm, drawing from consequentialist ethics. By applying procedural normative ethics, Manners suggests that the EU's foreign policy should be guided by principles acceptable to both Europeans and non-Europeans, enhancing the flexibility and relevance of NPE (Manners 2008:60). Another common criticism targets the EU's decision-making abilities and the lack of cohesion among its members, which could weaken the EU's status as an actor and consequently its influence (Puetter and Wiener 2007:1085). This falls in line with the same issue that Diez and Pace (2007:9) highlight – the fact that the norms the EU wants to uphold may not always align with each other and sometimes appear as competing.

3.4 Market Power Europe as an Alternative

Chad Damro argues that the EU can best be understood as a Market Power Europe (MPE) that exercises its authority through the externalisation of economic and social policies and regulatory frameworks related to market activities (Damro 2012). Damro's conceptual framework builds on the existing debates of European power discussed earlier in this chapter (Damro 2015:1339). Although diverging from them, and thus also from NPE, Damro's framework emphasises aspects not entirely different from the logic of NPE. The framework can thus potentially work as a complementary explanatory model in the study of the EU's cybersecurity strategy. Like Manners' assertion that the EU possesses a normative foundation (core and minor norms) that inclines it towards normative behaviour, Damro contends that the presence and interplay of three characteristics predispose the EU to operate as a MPE (Damro 2012:686). These characteristics are market size, regulatory institutions, and interest contestation.

The European single market represents the EU's material existence in the international system. It is thanks to the size of the market that the EU can externalise its policies and regulatory standards (ibid). Market size is crucial for two reasons regarding the externalisation of internal regulations. Firstly, it impacts governments' material incentives for coordinating regulatory standards. Secondly, it influences perceptions of outcomes by other actors. Additionally, market powers can intentionally or unintentionally coerce states to switch standards through economic pressure. A large market can alter others' beliefs about possible outcomes, attracting them to align with its preferences. Thus, the EU, with its substantial market size, wields influence by shaping both material incentives and perceptions in the international system (ibid:686-687). The EU as a regulatory institution is built on the idea that the Single market has institutional features that help determine the roles and interaction of several actors and provide the EU with regulatory capacity for being able to externalise policies and regulations. The EU's identity encompasses its institutional qualities and relies heavily on its institutional capacity to externalise regulatory measures (ibid:687). Furthermore, the Single market serves as a space where competing interests influence the likelihood of the EU exerting its power in external affairs. MPE's strategy for externalizing regulatory standards could thus be dependent on the varying degrees of influence exerted by particular interest groups (ibid:688). Damro's idea of externalisation can be divided into two stages. The first

involves EU institutions and actors striving to make other parties adopt regulatory standards akin to those in the European single market or to align their behaviour with the EU's market-related policies and regulations. The second stage is that the targets, usually non-EU entities, comply with the level of regulation. This two-stage process thus entails evaluating both the efforts to externalise and the actual achievement of such externalisation (ibid:690). Comparisons can be drawn with NPE and the analysis of what level of normative change the EU has managed to induce.

Damro himself raises the debate between NPE and MPE when he concludes that the best way to evaluate them is to study whether the EU influences the behaviour of others through norms or by externalisation of regulatory measures and market-related policies (ibid:697). MPE is thus a conceptual framework rather than a theory and can contribute to theory testing (Damro 2015:1340). Even though originally focused on market-related policy areas, MPE is not limited to policies directly linked to the EU's internal market. For example, the EU can still be understood as a security actor (ibid:1346), which could make the framework useful to this study of cybersecurity. This will be further discussed after the analysis in Chapter 6.

In earlier stages of this dissertation, the idea was to include the theory of neorealism as a potential explanatory model to contrast NPE. Neorealism could have been an alternative theory considered due to its emphasis on states' self-interest and power dynamics in international relations. However, neorealism tends to focus primarily on military capabilities and security concerns (Hyde-Price 2006:220), often overlooking the role of norms and values in shaping actors' behaviour. This can be seen as both an advantage and a factor that complicates the analysis. This thesis very clearly treats the EU as an entity, and it does not examine the intergovernmental structures needed for a neorealist approach. In contrast, MPE offers a perspective that complements NPE by highlighting the EU's influence through economic and regulatory frameworks, which aligns better with the general objective of the thesis as well as the research method.

3.5 Operationalization of NPE – a framework by Niemann and de Wekker

Sjursen (2006b) suggests conducting more comprehensive empirical studies to delve into whether the EU genuinely operates based on norms or primarily in its self-interest. She points out that the term Normative Power Europe lacks clarity, especially when it comes to defining specific criteria and standards for analysing the concept empirically. This section will lay out the choice of operationalization of NPE that will be used throughout this research. It is hoped that this research will make a valuable contribution by fulfilling the need for expanded empirical investigation as advocated by Sjursen, while also addressing many of the criticisms levelled against NPE as discussed earlier. Niemann & de Wekker (2010) respond to the uncertainties on how to apply the concept to empirical research. They tackle the questions of how one can identify normative power, what criteria qualify an action as normative power, and how can we observe and, to some degree, measure it. Doing so, they divide the operationalization into three levels: normative intent, normative process, and normative impact. This is the framework that will be used and below is thus an explanation of the framework.

Normative intent refers to how serious and genuine the EU's normative commitment is. For the EU to be a real normative power, the EU would need to be inherently normative, driven by the norms themselves rather than by self-interest. Exploring this dimension can provide insights into the authenticity of the EU's commitment to norms (Niemann & de Wekker 2010:7). The following questions are suggested to reveal this normative intent.

a) It is necessary to ask whether the EU/universal norms are central to the relation with the third country or rather are peripheral. If the norms seem to be prioritised, a genuine normative intent is likely (ibid:7-8).

b) Secondly, the norms promoted should be looked at in relation to EU interests, whether the norms advocated by the EU serve or hinder its interests. If norms contradict self-interest, it suggests their significance as they are upheld despite potential political or economic costs. Prioritising specific norms over interests can show a genuine normative dedication. Additionally, observing instances where the EU promotes norms despite

strong opposition or conflicts with other OECD states can refute claims of cultural imperialism, reinforcing the legitimacy of EU normative power (ibid:8).

c) A third important aspect is to ask whether the EU is acting consistently and if the EU is projecting a double standard. If a double standard can be identified, a conclusion may be drawn that the norms are not the most important basis in decision-making. Consistency refers to whether the EU applies different standards on the third country than internally, the same or different standards for different third countries, and whether standards and norms are followed up by actual foreign policy deeds and actions (ibid).

d) Lastly is coherence, which according to Niemann & de Wekker goes beyond consistency. Coherence is about how actions or claims are connected by shared principles. If there's inconsistent behaviour or application of norms, it's only considered incoherent if it can't be explained by a reasonable distinction. The authors suggest that policies can be justified by utility, values, or rights, and having coherence between these justifications adds legitimacy. Considering the understanding of normative intent, arguments based on values and rights seem more aligned with normative power than those based on utility (ibid).

Normative process refers to the extent to which an inclusive and reflexive foreign policy is pursued by the EU (vs. an 'our size fits all' approach). This is based on the idea that if the EU is to be seen as a" force for good", it is necessary to include external input and a reflection of the impact of the EU's actions (ibid:9). Furthermore, it is imperative to steer clear from of a "our size fits all" approach (Bicchi 2006). To prevent Eurocentric tendencies, the EU needs to promote universal norms, ones that align with the broader framework recognized by the EU framework (ibid & Manners 2008).

To avoid this, a normative power should be ready to adjust EU policy and norm promotion based on the specific context. This could entail, for instance, a readiness to adapt behaviour in response to more compelling arguments and to modify policies accordingly, taking into account the resulting implications. How can the degree of such reflexivity be measured? Niemann & de Wekker propose that it can be examined by assessing the extent to which EU external actions are based on a deliberate effort by EU decision-makers to critically analyse the expected outcomes and adjust the proposed actions accordingly.

Here, "conscious" refers to behaviour that is not routine based; instead, it involves practices that are actively considered and adapted, rather than relying on symbolic or ritualised actions. For instance, if EU foreign policymakers routinely apply certain templates or blueprints to partner countries without considering their specific circumstances, this is routine-based behaviour. Conversely, if the EU consciously evaluates its policies through external reviews or consultations and adjusts them accordingly, it demonstrates reflexivity (Niemann & de Wekker 2010:9). Inclusiveness is another criterion that needs to be considered. This is referred to as the difference between “giving voice to” and “speaking for” others (Bicchi 2006:289). The question is thus whether the EU considers the perspectives of those who will be impacted by its actions (Niemann & de Wekker 2010:9).

Normative impact refers to the development of norms in third countries and the importance of the EU’s normative power to be measured in relation to the actual normative impact. To do this, one needs to ask two questions; has any normative change occurred and was this change induced by the EU? (Niemann & de Wekker 2010:10). Starting with the first question of normative change, it is something that only can be approximated. Niemann & de Wekker suggest a discursive way of investigating this. One way is to study the extent to which the norms advocated by the EU are being discussed in the political and media discourse of the partner country, and how they become integrated into the prevailing discourse. Incorporation of norms into the discourse, for example, manifested by political actors referring to the norms, could thus be an initial indication of norm adoption. If norms are consistently attributed the same significance and meaning across various contexts and platforms, it suggests that relevant actors genuinely uphold these norms. This could be examined, for example, by analysing speeches of influential politicians from the partner country. Furthermore, it is important to evaluate whether and to what degree the legislation of the country has been revised to align with the norms promoted by the EU. For the second question, it is crucial to recognize that influences on the third country's normative change may extend beyond the EU to include other actors, such as international organisations or additional third countries. To investigate this, one can study whether the norms discussed are linked to the EU or another entity. Additionally, it is important to determine whether norms changed following the EU's normative engagement in the country or if they were already in place beforehand (ibid:11).

It is worth highlighting that the possibility of assessing the EU's normative impact in third countries is more limited compared to the assessment of normative intent and process. This is because the material of this thesis comes from the EU and thus risks showing a biased perspective. Niemann & de Wekker suggest that one approach is to look at the third country's domestic politics and media to get a sense of the discourse. This is not possible for me because of the language barrier. However, it is still possible to discern attitudes, opinions, and statements from some of the cyber dialogues that are studied. Considering these constraints, I must settle for the fact that the normative change can only be estimated, but that more in-depth analysis for each partner country is necessary to get a complete answer. After all, this is something that Niemann & de Wekker also recognize.

4. Research Design and Method: A Case Study Approach to the European Union Cybersecurity Strategy

4.1 Case Study

To find out whether the EU can be considered a normative power within cybersecurity, the research is conducted with case study as the chosen research design. Case studies enable an in-depth examination of political phenomena, with rich textual description (Halperin & Heath 2020:170). This therefore suits the purpose of this research that looks specifically at the EU's Cyber Security Strategy from a normative perspective. Case studies are fruitful for the application of theory from one context to another in order to test its accuracy in the new context (ibid). This is relevant for this research in which NPE is applied to the case of EU and cyber security which has been identified as a current gap in previous research. This aligns with Geddes' (2003) criterion of case studies that stipulates that the cases utilised to test arguments should differ from the cases that originally inspired those arguments. This ensures that each case study serves as a fresh evaluation of the theory. By doing this, such a test will hopefully contribute to the development of new knowledge either in favour or against NPE (ibid). The resulting knowledge from this research can then hopefully be used to draw some general conclusions within wider academic debates that can be useful in future research in cyber security governance and/or within the research field of NPE. As stated previously, NPE, founded by Manners and further developed by Niemann and de Wekker, is the theoretical starting point for this research. The research thus takes a deductive approach, meaning that instead of starting with and favouring observation, the research aims to formulate hypotheses based on established facts or initial theoretical assumptions (Hay 2002:30). It is thus the theory that guides the research and not the other way around. The aim is to move from a broader conception of NPE to specific observations. In that process, it typically begins with a theory that has already been validated or with a logical argument, and then extracts the significance or implications this holds for explaining a particular case or phenomena (Halperin & Heath 2020:33).

4.2 Qualitative Content Analysis

This research is conducted using a qualitative content analysis. Qualitative content analysis operates under the premise that it is feasible to unveil the connotations, intentions, and objectives within the text, and thereby "infer valid hidden or underlying meanings of interest to the researcher" (Weber 1990:72–76). Content analysis allows for evidence of what the actors are thinking and what their intentions might be (Halperin & Heath 2020). That is helpful in this research that wishes to uncover the normative actions of the EU within cybersecurity. A content analysis thus enables a systematic analysis of the chosen material to find clues for attitudes and intentions of the EU in this field. This research treats a whole text as a unit of content, meaning that the chosen documents will be studied in their entirety (ibid:378). Furthermore, as stated by Holsti (1969:14), "content analysis is any technique for making inferences by objectively and systematically identifying specified characteristics of messages". Thus, a content analysis can be either quantitative or qualitative. However, this research predominantly adopts a qualitative approach, aiming for an interpretive exploration to uncover intentions and motives within various textual sources related to the EU (Halperin & Heath 2020:365). As Drisko (2016:84) points out, this cannot always be done extensively by relying solely on word frequency counts as the analytical approach. The simplification involved in quantifying data in that way might not fully capture certain nuances of meaning. Quantifying content generally reveals the manifest content of a text, meaning content that can be observed easily, for example by counting the frequency of specific words (Halperin & Heath 2020:376). This research includes elements of such quantifying strategy in the analysis where occurrences of specific words and concepts are analysed (see codebook in 4.3). However, this research is mainly concerned with the latent content of the empirical material, therefore a qualitative approach dominates the analysis. A latent content analysis is more sensitive to the context surrounding the creation of texts, thereby offering better insights into meanings, norms, purposes, values, and motives (ibid 2020:365).

Another conceivable method thought for this research is discourse analysis. Discourse analysis focuses on the elements and structures of speech and primarily examines natural communication events, focusing on aspects like speaker turn-taking, propositions, and speech forms (Drisko 2016:82). What makes content analysis a more suitable option is

however that it focuses on the meaning of the text. Another general advantage of using content analysis is that the researcher can obtain material on decision-making without having to conduct interviews with the relevant actors involved. Researchers have the capability to examine statements made by officials to discern evidence about their perspectives and attitudes. Instead of relying solely on the recollection or selective disclosure of information by government officials regarding public hearings, researchers can analyse transcripts directly for a more accurate understanding (Halperin & Heath 2020:374). Content analysis can be a method for testing theory (Drisko 2016:86) which applies well to this research that aims to test NPE in the case of the EU's cybersecurity strategy.

Interestingly, researchers in the qualitative content analysis literature adopt different epistemological approaches. Some adopt a positivist or realist epistemology focusing less on interpretation, whereas researchers such as Mayring (2000) lean more towards a constructivist epistemological standpoint, highlighting the significance of researcher interpretation (Drisko 2016:88). For the validity of this research, it is important to set out the ontological and epistemological approach guiding the process. Ontology explores the fundamental nature of reality, focusing on the structure of the social world and its constituent elements. In political research, ontological inquiries delve into whether the social world differs fundamentally from the natural world and whether it exists objectively or is largely subjectively constructed. Epistemology, on the other hand, investigates the nature of knowledge itself—what can be known about social phenomena and what forms of knowledge are considered valid and credible in understanding the social world (Halperin & Heath 2020:28). The constructivist approach believes that the social and political realm is not fixed but is rather an inherently intersubjective space, shaped by social construction. There is no objective social or political reality that exists independently of our interpretation of it—there is no social sphere that exists apart from human activity (Hay 2002:199). Furthermore, constructivism highlights the influence of domestic norms on global politics and the impact of international norms on domestic political dynamics (ibid) which is part of what this research is focused on. Social phenomena and their interpretations are constantly shaped by the actions of social actors. This suggests that social phenomena and categories are not only constructed through social interaction but are also subject to ongoing revision (Bryman 2012:33).

In terms of epistemology, this study adopts an interpretive stance, positing that comprehension of the social realm can be achieved through the interpretation of the meanings that underlie human actions. Instead of aiming to explain and predict social phenomena using laws, the main objective of social science should be to comprehend human behaviour by interpreting the meanings, beliefs, and ideas that motivate people's actions (Halperin & Heath 2020:5). This highlights the divide between the focus on solely explaining human behaviour, which is central to the positivist approach in social sciences, and the emphasis on also understanding human behaviour (Bryman 2012:28).

A challenge with the conducting of content analysis lies in the importance of validity, replicability, and transparency. It is of high importance that a thorough content analysis relies on a systematic method that is clearly outlined for readers and can be replicated by fellow researchers (Drisko 2016). Furthermore, it is nearly impossible to construct a coding scheme that doesn't include at least some interpretation of the researcher (Bryman 2012:306). These issues and challenges are further elaborated upon in the section below.

4.3 Coding

Content analysis involves coding the content of the chosen material. Schreier (2012) emphasises coding as pivotal in qualitative content analysis, aiding researchers in identifying and summarising key meanings from diverse texts to address research questions. This coding process can generally be divided into three stages. The first stage consists of creating a protocol for identifying the target variables and categories. This stage is vital for ensuring the reliability of the coding, meaning that the coding can be done consistently throughout the text and be repeated in the same way. The second phase is the creation of codes for each variable that will signal their presence in the text. The third and last step is to code the material using this protocol and codes. This research will mostly apply priori codes or "closed coding", meaning that the codes are based on previous research and theory from which the categories are derived. However, a part of the coding is derived from reading the material to match the categories and codes correctly within the field of cybersecurity. The method of closed coding is therefore combined with "open coding" where the codes emerge from the data as one reads it (Halperin & Heath 2020:380, Drisko 2016:89). The "open coding" is used in the early

stages of creating the codebook for discovering the EU specific interests within the field of cybersecurity. The conducting of this research consists of two stages. In the first stage, the material is coded against the predetermined codebook using the software called Atlas. ti. Atlas. ti is a qualitative data analysis tool that facilitates close reading and analysis of documents. The results are thereafter compiled thoroughly in a separate document which allows to perform the final analysis of the results manually.

As briefly discussed in 4.2 it is of importance that the researcher evaluates the effectiveness of coded data in addressing the research question, and thereby the validity of the research. Given the contextual and latent nature of coding in qualitative content analysis, it is crucial to create a transparent map demonstrating how codes were deductively developed and applied (Drisko 2013). The categories and associated codes are derived from Niemann & de Wekker's framework as explained in 3.5. The detailed coding scheme guiding this research is presented below.

Category	Sub-category	Definition	Code
NORMATIVE INTENT	Central/peripheral values	Are norms at the centre or the periphery of the cybersecurity arguments of the EU? Prioritized values are an indication of normative power.	Peace Liberty Democracy Rule of Law Human rights Social solidarity Anti-Discrimination Sustainable development Good governance
	Self-interest	How do EU-promoted norms relate to EU interests? Prioritizing norms over interests shows genuine normative commitment.	Industry Critical Infrastructure Cyber Resilience Digital Single Market Combatting Cybercrime Data Privacy Innovation & Research International Cooperation Digital Supply Chains

	Double standard	Is EU acting consistently or not, meaning if EU applies the same or different standards on third countries as internally?	Human rights violation/abuses Condemnation International law Rule of law
	Coherence	Are actions or claims connected by shared principles? Arguments based on values and rights are more indication of normative intent rather than arguments based on utility.	International law Legal rights Treaties Human rights Fundamental rights Best interest Maximising efficiency Greater good Strategic Goals Economically Advantage Benefits Interests
Category	**Sub-category**	**Definition**	**Code**

NORMATIVE PROCESS	Reflexivity	Is EU ready to adjust policies if presented with better arguments? If EU can consciously evaluate its policies to fit the external context, it demonstrates reflexivity.	Stakeholders Consultation Actors Partner countries Civil society Experts Collaboration Partnership Impact Assessments Consequences Adaptation Outcome Adjustments
	Inclusiveness	Is EU considering the perspective of those being affected by the policies?	Civil society Working groups Forums Inclusion Capacity building Locals Power
	Universal norms	Universal norms refer to norms acknowledged by the UN or other institutions, not just the EU.	Budapest Convention UN
Category	**Sub-category**	**Definition**	**Code**

NORMATIVE IMPACT	Normative change	Did any normative change occur and was this change induced by the EU?	EU laws National legislation Reforms EU standards EU norms EU initiatives EU directives Project Change

Table 1. Represents the codebook guiding the analysis, derived from the framework of Niemann & de Wekker (2010:6-12).

4.4 Material and Limitations

The EU 2020 Cybersecurity Strategy (EUCSS) is extensive and wide-ranging. It consists of several initiatives, policies, and goals. Considering that this research aims to study the latest EUCSS from 2020, the material is limited to the years 2020 up until 2024. More specifically, the 2020 strategy was released on the 16th of December 2020, and this will thus mark the starting point for the research scope. This choice is motivated by the ambition of this research which is to unveil the EU's normative aspirations in the field of cybersecurity today. The aim is not to conduct a longitudinal study or compare different strategies, thus only the latest strategy is of relevance. The research has purposely left out specific initiatives within the 2020 EUCSS that target investments and policies for EU member states. Since the purpose is to find out to what extent the EU can shape what is considered normal outside of the EU, projects within the union are of less importance. To fully catch the EU's ambitions within the field and be able to answer my research question, the material is divided into two categories. The first set of materials is selected from material by the EU that represents the general objectives of the EU within the cybersecurity strategy. First and foremost, this includes the "Joint Communication to the European Parliament and the Council - The EUs Cybersecurity Strategy for the Digital Decade" (EC 2020b). Additional strategy documents and press releases are included from the European Agency for Cybersecurity (ENISA). This category of material is not limited to a specific sector within cybersecurity. A broad approach to the material is useful in the

sense that it allows for the revelation of the overreaching objectives and goals of the EU in cybersecurity and thus also hopefully can unveil the normative ambitions. A second set of materials is selected from the external engagements within the 2020 EUCSS. This choice is motivated by NPE that focuses on the EU's international role and relations with third countries, i.e., countries outside of the EU. The task is therefore to study the normative intent and diffusion of norms from the EU vis à vis third countries. Because of this, the second group of material is chosen from the externally focused initiatives by the EU that highlight the need for international cooperation. This is represented by material on several worldwide CCB projects carried out in cooperation with the EU and the Council of Europe. Ongoing projects include iProceeds-2, CyberEast, and CyberSouth. The project objectives of these activities are therefore included as indicators of the EU's external efforts in promoting its cyber norms. Material from several cyber dialogues between the EU and partner countries is also included. Cyber dialogues between the EU and Korea, the USA, China, and Ukraine are analysed. Based on the above-mentioned structure, a total of 17 documents constitute the material for the empirical analysis.

5. Analysis: Normativity Explored

5.1 Normative Intent

The first criterion that the EU needs to fulfil to be a normative power within the field of cybersecurity is one of genuine normative intent. As explained by Niemann & de Wekker (2010), this requires that the EU's policies are normatively driven and motivated by norms and values rather than self-interests. The EU attaches great importance to explaining the importance of norms and values within its cybersecurity strategy. What is evident however is that the five core norms appear to a much larger extent compared to the minor norms. This may not be surprising, however, considering that the core norms are derived from the very core of the EU's raison d'etre. The joint communication of 2020 EUCSS (EC 2020b) puts values at the centre to a larger extent than other policy documents do. The first page of the strategy highlights the importance of the Rule of Law, fundamental rights, freedoms, and democracy and explicitly state them as core values of the EU (EC 2020b:1). Their centrality indeed suggests a strong normative intent but must be backed up by demonstrating the centrality of the values in practice. Furthermore, it becomes apparent from the dataset that values are not always explicitly stated; however, a close reading often reveals a normatively driven argument implicit within the text

5.1.1 Values

An example of this is peace which is never expressed in that form. In the Council Conclusion, peace is highlighted through the emphasis on preventing cyberattacks and maintaining stability in cyberspace. Words such as "stable" and "secure" can be assumed to allude to stability and peace in cyberspace and within cybersecurity.

> "STRESSES that the cyber posture aims to combine the various initiatives that concur in EU actions consolidating peace and stability in the cyberspace and in favour of an open, free, global, stable and secure cyberspace" (Council of the European Union 2022:5).

Liberty and freedom are often indirectly referenced in the focus on enhancing cybersecurity without compromising fundamental and individual freedoms, including privacy and personal data protection (Council of Europe 2022a).

> "Mindful of the need to respect fundamental rights and freedoms, including the protection of individuals with regarding to the processing of personal data, when protecting society against crime" (Council of Europe 2023:3).

As for democracy, the implication of a commitment to defending democratic principles against cyber threats is more inferred from the general context of discussing cybersecurity. Often, the importance of collective action and solidarity in addressing cyber threats is emphasised, which indirectly aligns with the defence of democratic values. However, when describing the cybersecurity threat landscape, attacks against democratic institutions and electoral processes are highlighted as a risk factor (Breton 2023b).

> "We are not talking anymore only about well-known malware but also about cyber as an economic or military weapon, used to disrupt supply chains, threaten critical infrastructures, disorganize our societies, attack our democratic institutions and electoral processes, or simply spread disinformation" (Breton 2023b).

But overall, it is possible to discern a trend where democracy does not occur to the extent that might be expected considering its centrality in the 2020 EUCSS strategy document. There, it is almost exclusively mentioned in reference to the European Democracy Action Plan and the need for building more resilient democracies within the union. This is in the context of the growing amount of malicious cyber activities threatening the democratic systems of EU societies (EC 2020b:6). Rule of Law is generally highlighted by the emphasis on upholding international law and the rules-based international order in cyberspace. Rule of Law is most often expressed together with human rights and fundamental freedoms. The notion of the Rule of Law is central throughout the strategy document (EC 2020b) and is usually discussed together with human rights as important values for the EU's vision of a cyberspace model. Rule of law occurs in all the project objective summaries, indicating its importance independent of what region the project concerns.

> "The adoption of complete and effective legislation that meets human rights and rule of law requirements remains a strategic priority" (Council of Europe 2023:6).

Good governance is generally implicitly referenced in the call for cooperation and coordination at the EU level to address cyber threats effectively. For example, good governance is implied through the focus on enhancing cybersecurity capabilities and crisis management mechanisms (Council of the European Union 2022).

As previously discussed, the occurrence of minor norms is much scarcer. Looking solely at the strategy document, it is safe to say that the core values of the EU seem to be important, whereas the minor norms are of less importance. Among the core norms, all are recurrently mentioned in the strategy document except for peace, while among the minor norms, only sustainable development is represented in the text. Solidarity is particularly evident in the speeches where the importance of collective action and solidarity in addressing cyber threats is emphasized (Breton 2023a). Social solidarity is indicated through the proposal of a European Cyber Reserve to provide mutual assistance in the event of cyberattacks. Furthermore, a discernible theme emerges from the recent material, where expressions of solidarity are prominently featured in the discourse supporting Ukraine. The discourse around this topic is shaped in a way that highlights the need for support and solidarity with Ukraine - where the protection of critical infrastructure is an area where the EU can aid Ukraine in its resilience. It is worth noticing that this is expressed in the EU-Ukraine cyber dialogue, where the setting and context must be considered. However, social solidarity seems to be part of the EU's overall approach as well since social solidarity is implicitly referenced in the call for cooperation and solidarity among EU member states and partners to address cyber threats collectively (Council of the European Union 2022).

Whereas the strategy document covers nearly all of the core norms and values, it is possible to identify contexts where this is not the case. Naturally, the strategy document wants to declare all the cybersecurity objectives in a broad sense. To what extent this is backed up in practice could potentially be a different story. The set of material covering the EU's external cybersecurity engagements thus becomes extra important in this regard. For instance, core values that occur in the CyberEast project are limited to human rights

and the Rule of Law where they are highlighted as equally important. Other core values of the EU are however not explicitly mentioned. In the speech covering the enhanced EU-Ukraine cooperation in cybersecurity (EC 2023a) no values are mentioned at all. In general, it seems to be a pattern where cyber dialogues tend to refrain from including values and norms. This is true also for the EU-US dialogue where fundamental freedoms and human rights are briefly mentioned in the introduction but not elaborated on further throughout the dialogue (EC 2023b). Similarly, in the speech at the High-Level Conference on Cybersecurity in the Republic of Korea (Breton 2023b), they are only mentioned on one occasion which is in the concluding remarks of the speech. There appears to be a difference in what is expressed and advocated for in the strategy and what is communicated directly to international partners. While this can be considered a sign of the EU projecting a double standard, it could also be indicative of reflexivity, something that will be further discussed in section 5.2. Interestingly, ENISA's international strategy is completely lacking any references to the core values. It is explicitly stated that ENISA's international cooperation will prioritise partners aligned with EU values (ENISA 2021:5). However, aside from this reference, the document lacks further mentions of values. It is difficult to determine the reason for this, but it undoubtedly seems to be differences in what the European Commission expresses in the joint communication and what ENISA sees as its international objective guidelines.

5.1.2 Self-interests

Before drawing any conclusions on the centrality of values it is necessary to study them in relation to the EU's interests. As the theoretical framework establishes, the norms being promoted should always be looked at in relation to self-interests. The idea is that if norms are prioritised despite contradicting the EU's self-interests, it would be indicative of a genuine normative intent. When studying the 2020 EUCSS it becomes clear, just as Niemann & de Wekker discuss (Niemann & de Wekker 2010:7), that there is no value in trying to identify a dichotomy of norms versus interests. Just as Diez (2005:624) suggests, one can assume that self-interests and normative ambitions go hand in hand. The 2020 EUCSS revealed this since it was evident how interests and norms run in parallel above anything else. That said, the analysis primarily aimed to discern whether values or interests are central to the arguments and opinions expressed by the EU. Although one

does not exclude the other, it can still serve as an indicator of genuine normative intent. The determination of what interests are important for the EU within the field of cybersecurity was inductively identified in the early stages of the research in the process of creating the coding scheme. The results of the coding reveal a widespread in what interests are highlighted and what space they are given. Concerning the strategy document in relation to infrastructure, it appears that the EU prioritizes the norms and values of democracy and liberty over the EU's interest in infrastructure. The emphasis is on protecting fundamental rights, ensuring the Rule of Law, and promoting international security and stability, even in the face of threats to infrastructure (EC 2020b:2). Regarding innovation, the EU recognizes the importance of both democracy and liberty in safeguarding fundamental rights. At the same time, the text emphasises the critical role of innovation, connectivity, and automation for the economy, society, and global development (EC 2020b:4). Both sets of values are considered essential, with cybersecurity serving as a bridge between them to ensure that innovation can thrive while protecting fundamental rights and promoting international security and stability. There is thus no contradiction between the two, but rather an idea of their mutual importance. Cyber resilience, data privacy and protection of supply chains are discussed hand in hand with the EU's core values and there is no indication of the values being prioritised at the cost of EU interest. Quite the contrary as they rather seem to be reinforcing each other.

International cooperation and data privacy are great examples of this. In the 2020 EUCSS, cooperation can be considered a mixture of a norm and an interest of the EU. Throughout the dataset cooperation is the code with the most frequency. There is no doubt that cooperation is important for the EU in the governance of cybersecurity. It is used as a concept that permeates the whole strategy. Cooperation between EU member states is expressed as vital in order to secure safe cybersecurity in the Union. International cooperation with third countries is however also strongly encouraged. As expressed by ENISA:

> "ENISA will focus its international cooperation on partners with which the Union has strategic economic relationships, and which share the Union's values" (ENISA 2021:5).

The EU's call for closer cooperation with allies like the United States and NATO on cybersecurity demonstrates its interest in fostering collaborative efforts to address global cyber threats. By promoting international cooperation and information sharing, the EU seeks to bolster its cyber defences and enhance collective security in cyberspace (Breton 2023a). When the EU suggests establishing a strategic collaboration in the cyber realm with key allies such as the Republic of Korea, it is an initiative to advance a secure cyberspace on a global scale. It underscores the EU's commitment to enhancing international partnerships to tackle cybersecurity challenges worldwide and advocate for responsible conduct in cyberspace (Breton 2023a). The resumption of the EU-China High-level Digital Dialogue (EC 2023c) indicates a commitment to cooperation and engagement, even in areas where disagreements exist. This aligns with the EU's normative power in fostering dialogue and collaboration to address common challenges and achieve mutual benefits. The EU's interest in international cooperation often overlaps with its interest in combatting cybercrime. The importance of international cooperation is emphasised as important for addressing cybercrime and enhancing cybersecurity (Council of Europe 2021, Council of Europe 2023).

As previously discussed, the protection of data privacy overlaps largely with the protection of the Rule of Law, fundamental rights, and freedoms. Discussions of the Data Governance Act and the Data Act, which include provisions to protect data privacy and sovereignty, reflect the EU's interest in safeguarding personal and sensitive data (Breton 2023a, Council of Europe 2022a, Council of Europe 2021, Council of Europe 2022b). Data privacy is also highlighted in the context of the protection of children against sexual violence (Council of Europe 2023).

Industry and critical infrastructure are often discussed together and in the context of the importance of protecting them from cyber threats and ensuring their operation and resilience (Breton 2023a, Breton 2023b). Commissioner Breton highlights initiatives aimed at establishing stringent standards applicable across key economic sectors to bolster their resilience against cyber threats. Additionally, the proposal includes minimum cybersecurity standards for products entering the EU market. These actions are motivated by the EU's commitment to protecting its industries and vital infrastructure from cyber threats (Breton 2023a). The EU furthermore highlights the increasing risk of cyber threats targeting various industries, including critical infrastructure, supply chains, and

intellectual property. The EU's cybersecurity strategy aims to protect these industries from cyberattacks, which aligns with its interests in maintaining economic stability and competitiveness.

> "EMPHASISES that malicious behaviour in cyberspace, emanating from both State and non-state actors, has intensified in recent years, including a sharp and constant surge in malicious activities targeting the EU and its Member States' critical infrastructure, supply chains and intellectual property, the increased risk of spillover effects as well as a rise in ransomware attacks against our businesses, organisations and citizens" (Council of the European Union 2022:4).

What could be said for some cases is that EU interests are mentioned explicitly to a larger extent compared to the values. This is especially the case in the dialogues between the EU and several third countries. The protection of critical infrastructure was especially prevalent in the dialogue between the EU and the US and seemed to be a high priority in their discussions. Critical infrastructure, resilience and supply chains are among the most discussed interests that the EU and the US wish to strengthen (EC 2023b). A similar stance is visible in the dialogue between the EU and Ukraine where there seems to be a larger focus on the EU's interests than on norms. The dialogue between the EU and China had a large focus on interests compared to values. The dialogue prioritises interest over values - though there aren't any interests that necessarily go against those of the EU's core norms. What is interesting however is that economy and market access are discussed, something that is not too apparent in communications with other third countries. The protection and enhanced resilience of critical infrastructure from cyber threats includes measures such as developing a high common level of cybersecurity across the Union, regulating digital operational resilience for the financial sector, and ensuring cybersecurity in institutions, bodies, offices, and agencies of the Union (Council of the European Union 2022). These efforts demonstrate the EU's commitment to safeguarding critical infrastructure, which is vital for its economic and societal functioning. These discussions shed light on the connection between cybersecurity threats and market priorities. Although normative aspirations characterize the EU's strategy, there remains a strong focus on economic aspects as well. Breton highlights the importance of cybersecurity for the digital single market, emphasising the need for harmonised security requirements across Member States. This underscores the EU's interest in ensuring a

secure and trustworthy digital environment to facilitate cross-border data flows and promote digital innovation and commerce within the single market (Breton 2023a).

> "We are raising the level of resilience and security within our single market through an ambitious technological and regulatory approach" (Breton 2023a).

The EU aims to ensure that its digital single market is cyber-secure. By proposing cybersecurity minimum requirements for products placed on the EU market, the EU seeks to create a secure digital environment, thus aligning with its interests in fostering the digital single market (Breton 2023a). The EU also calls for investment in innovation, research, and technological development to enhance the EU's technological sovereignty, including in the cyber domain. It emphasises the importance of making intensive use of new technologies such as quantum computing, artificial intelligence, and big data to achieve comparative advantages. These efforts align with the EU's interests in fostering innovation and maintaining its technological leadership in cyberspace (Council of the European Union 2022:7). There are also several mentions of practical considerations such as cost reduction, risk mitigation and supply chain resilience. The focus on economic impact is rather apparent, for example in the discussion of the millions of records lost through data breaches and the case related to this (EC 2020b:2) and the general annual cost of cybercrime to the global economy (EC 2020b:3).

> "Cybersecurity by design for industrial processes, operations and devices can mitigate risks, potentially reduce costs to companies as well as to wider society, and thereby increase resilience" (EC 2020b:5).

5.1.3 Coherence & double standard

For the EU to show genuine normative intent it must act in a consistent manner. To identify potential double standards, the externally focused material was cross-examined against each other. Based on the findings from that analysis there seem to be no signs of double standards based on the definition by Niemann & de Wekker. Even though the EU focuses on different topics in different third countries, there are no double standards in the sense that the core values are intentionally compromised. The EU is consistent in its efforts to combat cybercrime and enhance cybersecurity. While they address different regions, the standards and approaches outlined appear consistent in their goal of addressing cyber threats. There is a consistent emphasis on adherence to international law, particularly through the implementation of the Budapest Convention on Cybercrime.

However, some examples where the different focus is more apparent include the cyber dialogues. The EU-US dialogue does not make any references to human rights, democracy, or other core values. One possible explanation for this is that the US is among the partners closer to the EU on these issues, reducing the immediate urgency to discuss them. The dialogue between the EU and China emphasises cooperation on digital policies, including data regulation and AI governance. However, it does not explicitly mention the EU's approach to cybersecurity or cybercrime within the EU. If the EU emphasises cooperation with China on digital policies without addressing cybersecurity concerns, it could indicate a double standard in prioritising economic cooperation over cybersecurity. These dialogues can be contrasted with the CyberSouth project (Council of Europe 2021) which focuses more on the alignment with the EU and Council of Europe standards. A possible explanation for this is the region's aspirations for EU accession.

As laid out in 2.1, Carrapico & Barrinha (2017) and Pâris (2021) discuss coherence as a challenge for the EU within cyber governance. They argue that differences between Member states raise issues of different priorities and various approaches to cybersecurity. This problem is not evident in the research of this thesis. This is mainly due to the choice of material as well as the research purpose of the thesis. The material favours the European Commission and per the research question, the EU is analysed as one entity where the opinions or intents of individual Member states are not studied. This research applies coherence as interpreted by Niemann & de Wekker which is strongly related to

their concept of double standard. If a double standard was to be detected, coherence would refer to the way such double-standard actions are justified and explained by the EU. Since no evident double standard was found, neither incoherence was apparent. However, coherence in terms of what the EU's general arguments are based upon is central throughout the analysis of the dataset. Niemann & de Wekker state that arguments grounded in values and rights appear to better fit normative power compared to arguments that are based on utility. I argue that this is highly connected to the dynamic between norms and self-interests discussed previously, where self-interests get to represent the utility side of the EU's argumentations.

5.2 Normative Process

The second criterion that the EU needs to fulfil to be a normative power within the field of cybersecurity is one of normative process. It is important that the EU's external policies are reflexive and that the EU values external input. Being able to promote universally acknowledged norms is one side of reflexivity that Niemann & de Wekker argue is a prerequisite for normative power. Promoting universally acknowledged norms is however not enough to show genuine normative power. To strengthen the credibility of the EU being reflexive, the EU should also have the capacity to adjust its policies to specific contexts and be open to evaluate them. The notion of inclusiveness goes hand in hand with reflexivity and asks whether the EU considers the perspectives of those who will be impacted by its policies. This is essential to avoid acting in a Eurocentric manner. Like reflexivity, the involvement of other stakeholders such as civil society could be an indication of this.

5.2.1 Universal norms

The analysis shows that norms promoted are derived from the EU's treaties but do also have their basis in universally acknowledged norms in the UN framework. The EU frequently references UN norms and principles, suggesting a promotion of universal norms rather than ones limited to the EU. It is stated that the EU is committed to the universal UN framework of responsible state behaviour. Furthermore, the EU confirms the continuing promotion of the UN Cyber Programme of Action to help states implement the framework (EC 2023b).

> "The EU continues to work with international partners to advance and promote a global, open, stable, and secure cyberspace where international law, in particular the United Nations (UN) Charter, is respected" (EC 2020b:20).

EU reaffirms its commitment to the UN framework for responsible state behaviour in cyberspace by emphasising adherence to voluntary, non-binding norms of responsible state behaviour agreed upon by all UN member states. The EU stresses the importance of promoting a global, stable, and secure cyberspace where human rights, fundamental freedoms, and the Rule of Law fully apply. Additionally, the EU commits to engaging in relevant UN processes related to cybersecurity (Council of the European Union 2022).

> "STRESSES the importance of continued efforts to uphold and promote the UN Framework for responsible state behaviour" (Council of the European Union 2022:13).

Although not originating from the UN, the Council of Europe Budapest Convention on Cybercrime is very central in the 2020 EUCSS. This is the first international treaty seeking to address cybercrime and is thus not originating from the EU. Throughout the strategy documents, there is a section dedicated to the Budapest Convention where the EU expresses its ambition to support countries to accede to the convention (EC 2020b:21). The EU's promotion of the Budapest Convention can be seen as both important and symbolic in the global competition of cybersecurity governance. We know that opposing conventions have been proposed which both Russia, China, and India support. As discussed in 2.2, such an alternative treaty would threaten the fundamental

freedoms, human rights and democratic principles associated with the current Budapest Convention and the EU (Anagnostakis 2022:247, Pawlak 2016). This highlights the significance of the EU in expanding its involvement in a value-driven strategy, particularly with countries in the Global South. Considering this, one could argue that the EU's promotion of the Budapest Convention becomes a tool in a well-thought-out strategy that benefits the EU rather than being a result of a genuine normative driving force. Promoting the Budapest Convention becomes imperative to ensure that opposing countries do not gain excessive influence at the expense of the EU's authority.

5.2.2 Reflexivity

The results of the dataset regarding reflexivity are rather mixed. Evaluating the EU's reflexivity vis-a-vis third countries proved naturally challenging when analysing the strategy documents. However, it was possible to get a sense of the EU's general approach to the concept and analyse the overreaching discourse of how the EU evaluates its policies and their impact. Where reflexivity is most visible is in the EU's efforts to engage in consultation with different stakeholders. This is for example the case in the section of the 2020 EUCSS that discusses international standardisation.

> "Stronger cooperation and burden sharing should be sought with like-minded partners and European stakeholders" (EC 2020b:20).

This shows that the EU values cooperation and believes other stakeholders can contribute with valuable knowledge. A similar approach is taken in the discussion on preventing attacks on information systems, where the Internet Corporation for Assigned Names and Numbers (ICANN) is highlighted as an important partner (EC 2020b:15). Cooperation with third countries and multi-stakeholder community is emphasised to reach a coherent international cyber policy (EC 2020b:19).

Generally, the EU calls for cooperation with both partner countries, international organisations, and the private sector, and highlights the importance of stakeholder engagement during policy formulation to strengthen cybersecurity capabilities. This emphasis on collaboration suggests that the EU is receptive to input from various

stakeholders and considers their perspectives in shaping its cybersecurity policies (Council of the European Union 2022). A similar approach is evident in the projects targeting both the Southern and Eastern European region where activities such as regional workshops, conferences, and training events suggest opportunities for stakeholder engagement. The inclusion of representatives from judicial training institutions, law enforcement authorities, and other relevant stakeholders in these events could facilitate consultations during policy formulation (Council of Europe 2021). These forms of cooperation imply an awareness of the need to adapt policies based on the specific context and challenges, as well as a commitment to informed decision-making and evaluation of policy outcomes.

Information sharing is an important priority for the EU to increase knowledge about the cybersecurity threat landscape (EC 2023a). This sharing of information can be seen as a reflexive approach since the EU is willing to both receive and share information about best practices. Commissioner Breton mentions the importance of cooperation with strategic partners like the Republic of Korea in enhancing cyber resilience. He also emphasises the role of information-sharing and capacity-building exercises (Breton 2023b). Information sharing is also highlighted as vital between cybercrime units and financial units (Council of Europe 2022a)

Is the EU ready to adjust its policies based on potential new knowledge? The conduction of impact assessment is one way of answering this question. There are some occasions where the EU includes considerations of the impact of its policies. One of these instances concerns the EU 5G Toolbox where the EU considers the results of the report and based on those, encourages Member States to accelerate the work of completing the implementation of the Toolbox (EC 2020b:8-9).

> "In December 2020, the Commission published a report on the impacts of the Recommendation of 26 March 2019 on the Cybersecurity of 5G networks" (EC 2020b:8).

There is evidence of the EU not implementing an "our size fits all" approach, but rather adapting the policies according to the needs of specific countries and regions. In the iProceed2 project, for example, the EU makes clear distinctions between the needs of Montenegro, Serbia, and Türkiye. In Montenegro there exists a limited cybercrime and

digital forensics investigative capacity whereas in Serbia, for example, there is a need for more training of staff of the Special Prosecutor's Office of Serbia and Cybercrime Department of the Ministry of Interior of Serbia (Council of Europe 2022a:2). In the southern region, EU put great value in preparing assessments on legislation, data protection frameworks, and judicial training systems. These assessments indicate a level of reflexivity as they involve a critical analysis of the existing situation before proposing interventions. By evaluating the legislative and institutional landscape, decision-makers can better understand the context and potential implications of policy actions (Council of Europe 2021). EU highlights the need for doing several assessments in the Eastern European countries within different fields to identify weaknesses and needs for improvement.

> "Assessment of efficiency of cybercrime reporting systems (both public and industry-based) through in-country visits and advisory missions, with experience sourced from other capacity building projects run by the Council of Europe, with regional conclusions" (Council of Europe 2022b:8)

Just as the above quote signalises, this is done on a country-by-country basis. There is no ambition to apply an "our size fits all" but rather to evaluate the needs in detail. This is further showed in the objective of adopting legislative and policy frameworks compliant with the Budapest Convention, where activities include national seminars and working groups including national experts (Council of Europe 2022b:5). Another example is the EU-Ukraine cooperation that suggests that their Working Arrangement involves ongoing cooperation and adaptation, indicating a level of reflexivity in the EU-Ukraine cybersecurity efforts. The agreement mentions short-term cooperation actions and paves the way for longer-term alignment, suggesting a deliberate effort to adjust policies based on evolving circumstances (EC 2023a).

5.2.3 Inclusiveness

Common to much of the dataset is that the EU often does not explicitly state the importance of inclusiveness, but rather pushes for collaboration and cooperation in general terms. It is highlighted that the EU should expand its dialogues with third countries to share best practices with one another and develop more effective cooperation. These arguments are paired with an ambition to establish exchanges with other regional organizations, where the African Union, the ASEAN Regional Forum and the Organisation of American States are mentioned explicitly (EC 2020b:21-22). ENISA emphasises building partnerships with international organisations such as the OECD, OSCE, and NATO. These partnerships suggest a collaborative approach to addressing cybersecurity challenges, involving a range of stakeholders beyond the EU (ENISA 2021:7). The Council conclusions (Council of the European Union 2022) emphasise the importance of engagement with civil society organisations in policy dialogue. This suggests a recognition of the value of diverse perspectives and expertise beyond traditional government and industry stakeholders.

> "REITERATES its commitment to inform the public about cyber threats and the measures taken nationally and at the EU level against these threats by involving civil society, the private sector, and academia, with a view to raising awareness and encouraging an appropriate level of cyber protection and cyber hygiene" (Council of the European Union 2022:8).

Similarly, the Council conclusions (Council of the European Union 2022:8) mention the need for consultation with the affected in decision-making processes, suggesting to actively involve users. EU also aims to develop tailored CCB programmes for third states, indicating that they are not using an "our size fits all" approach (Council of the European Union 2022:14). There are indications of the EU seeing the need to work from a bottom-up approach and consider those that are being affected by the project and its policies. For example, it is explicitly stated that the activities should complement regional activities (Council of Europe 2022a:3). The focus is evidently on capacity building, particularly in strengthening national authorities (ibid:4). Looking at the general activities that should lead to expected results, there are several occasions of workshops and exercises involving national institutions. The EU-US dialogue (EC 2023b) stands out because the primary

focus is not solely on enhancing cybersecurity within the US with EU assistance, but rather on fostering cooperation between the EU and the US to enhance the global cybersecurity landscape. For example, they reaffirmed their cooperation in strengthening cyber resilience on a global scale. They also highlighted the need for supporting partner countries with capacity-building measures, including Ukraine, Moldova, Western Balkans, Africa, and Latin America. The dialogue includes discussions on the Organization on Security and Co-operation in Europe and the ASEAN Regional Forum, the G7 and G20, indicating that they see the value in consultation with other forums to get new perspectives on the issues.

While the EU acknowledges the importance of cooperation with Ukraine, it is framed within the context of EU-Ukraine relations and Ukraine's path towards EU accession. This could be interpreted as an EU-centric framing that prioritises the EU's interests and perspectives over those of Ukraine, potentially undermining the principle of inclusiveness in decision-making. However, an EU accession is both in the EU's and Ukraine's interest. However, there are citations from both Oleksiy Danilov (Secretary of the National Security and Defense Council of Ukraine) and State Service of Special Communications and Information Protection of Ukraine (SSSCIP) Chairman, Yurii Shchyhol. Both express their satisfaction regarding the new arrangement and refer explicitly to strengthened cooperation. One of the main priorities for the arrangements between the EU and Ukraine includes information sharing with a more systematic exchange of knowledge to strengthen local stakeholders and communities. This indicates that the EU indeed is attentive to the ones being affected by the policies and is working towards the improvement of their capacity.

In the Eastern European region, it is possible to discern a focus on involving both civil society and other actors with national expertise. This is mainly indicated by the number of national seminars and working groups being conducted within the project. There is a separate section of activities that aims to include civil society.

> "Cybercrime-centric public communication campaign jointly organized with local counterparts and donors on the occasion of important national and, where possible, at regional/international events under the project" (Council of Europe (2022b:7).

> "Cooperate with personal data protection authorities and national communications regulators to increase their role in ensuring trust and cooperation between public and private sector in terms of access to data in criminal cases" (ibid).

In the context of adopting legislative policies compliant with the Budapest Convention, there are activities including national discussion forums involving national policymakers (ibid:5). Nevertheless, it is inevitable to conclude that the EU does not show sufficient signs of inclusiveness in concrete terms. While the EU underscores the importance of cooperation and partnership in addressing cybersecurity challenges, there is in fact limited evidence of explicit engagement with civil society organisations, consultation with affected communities, or representation of diverse perspectives beyond governmental and strategic realms. The EU and the Council of Europe project in the southern region primarily focuses on activities involving government institutions, law enforcement authorities, and judicial training institutes. While these stakeholders play crucial roles, the absence of explicit mention of representation from diverse perspectives, such as those from the private sector, academia, or marginalised groups, raises concerns about inclusiveness. There is generally a lack of clarity regarding the engagement with civil society organisations, consultation with affected communities, and representation of diverse perspectives. Enhancing inclusiveness requires more explicit efforts to engage with a wide range of stakeholders, including civil society organisations, affected communities, and diverse interest groups, to ensure that their perspectives are adequately considered in policy formulation and implementation processes.

5.3 Normative Change

Is there evidence to suggest that the EU has influenced normative change in third countries? As suspected in 3.6 it was more of a challenge to study the category of normative change. While much of the dataset outlines significant efforts by the EU to strengthen cybersecurity both internally and internationally, it does not always provide explicit evidence of normative change in third countries as a direct result of EU engagement. Any changes can thus only be estimated as being the result of EU activity.

In southeast Europe and Türkiye, one of the results in the region is that "all the countries have completed the establishment of the Computer Security Incident Response Teams (CIRTs)/ Computer Emergency Response Teams (CERTs) or are in the process of expanding their operations" (Council of Europe 2022a:2). Furthermore, Cybil sets out all the outcomes of the project in which it is clear that the project has delivered some actual change. This includes strengthened legislation regarding securing electronic evidence and data access in line with data protection and the EU's rule of law requirements (Cybil 2024a). In the dialogues, there are indications of development towards normative change. The political discourse between the EU and Ukraine may indicate an initial stage of norm adoption or alignment. The dialogue mentions Ukraine's efforts to align its cybersecurity-related policies and legislation with the EU legal and institutional framework. This alignment suggests a convergence of norms between the EU and Ukraine in the field of cybersecurity. By adopting legislation that reflects EU standards and practices, Ukraine may be demonstrating a normative change influenced by EU norms and values. One example is that Ukraine provided updates on their efforts to develop their cybersecurity policies and legislation in line with the EU's legal framework (EEAS 2022).

The CyberSouth project (Council of Europe 2021) suggests that normative change in the Southern Neighbourhood countries are occurring because of the EU's normative engagement, particularly through its funded projects and capacity-building efforts. The emphasis on legislative reforms and alignment with international standards indicates that normative change is happening in response to the EU initiatives rather than being pre-existing. An example of normative change in this context is that Tunisia in March 2024 signed accession to the Budapest Convention after strong cooperation with the Council of Europe. According to the project, Tunisia had earlier been invited to accede to the

convention. Their accession therefore signalises a normative impact has taken place. Furthermore, as stated in the project, both Morocco and Tunisia have acceded to the Data Protection Convention 108 of the Council of Europe.

Previous projects within the eastern region from 2011 to 2014 are discussed where it becomes clear how these projects helped the countries in the Eastern Partnership to increase their capabilities to deal with cybercrimes, and that countries are now able to use the tools that they managed to develop during the projects. For example, the International Cooperation advanced information sections under the Octopus Cybercrime Community, standard templates for Article 29-30 (data preservation) and Article 31 (MLA requests for subscriber information) requests under the Budapest Convention. Furthermore, the previous projects helped improve the public-private cooperation frameworks (Council of Europe 2022b:2). There are more concrete examples where the EU has induced change. One example is Moldova which has initiated a digital transformation of public policy processes through the e-monitoring system. Utilizing advanced technology, will enable real-time tracking of national and EU-related commitments, aiding Moldova's European integration (EU4Digital 2023). Also, this year, Moldova took steps to align with EU standards, particularly the EU NIS Directive, when Moldova approved a draft law to strengthen cybersecurity (EU4Digital 2024a). In Georgia in June 2023, the parliament adopted the Law of Georgia on Personal Data Protection. This was a step in the process of fulfilling what was agreed on in the EU-Georgia Association Agreement to harmonise legislation with European standards related to data protection. This is thus a further example where the EU’s efforts lead to normative change (EU4digital 2024b).

6. Discussion: Explaining Normativity in the European Union's Cybersecurity Strategy

This thesis wanted to discover to what extent the EU acts as a normative power within cybersecurity based on its current cybersecurity strategy from 2020. As laid out in Chapter 3 there are alternative insights from MPE which potentially better can explain the EU's cybersecurity strategy. Based on the findings analysed in the previous chapter, a theoretical discussion of these findings is necessary to reach any conclusions about the EU's approach. Based on the findings, this thesis argues that the EU to a large extent acts as a normative power within cybersecurity, albeit with some limitations. Where the EU falls short in its normativity is regarding the occasionally prioritising of self-interest before values, and in a lack of concrete evidence of inclusiveness. The EU's self-interested tendencies align with a market-oriented approach asserted by MPE.

If one were to study only the EU's strategy documents and the EU's expressed normative ambitions, there is overwhelming evidence pointing towards genuine normative intent. The EU emphasises the importance of norms and values in its cybersecurity strategy, placing core values such as Rule of Law, fundamental rights, freedoms, democracy, and peace at the centre of its discourse. These values are evident in official communications and strategies, suggesting a genuine normative intent. Other norms may be implicitly referenced, but still indicate a normatively driven argument. However, as seen from the findings, values are sometimes less explicitly mentioned in dialogues with third countries where interests like protecting critical infrastructure or economic cooperation are more prominent. This is shown in the dialogue with the US where critical infrastructure is especially prioritised (EC 2023b), in the dialogue with Ukraine (EC 2023a), and in China (EC 2023c) where interests are generally given more attention than norms. Examining the 2020 EUCSS reaffirmed Niemann & de Wekker's argument (2010:7) that attempting to identify a dichotomy of norms versus interests is of little value. Aligning with Diez's perspective (2005:624), it is instead more accurate to conclude that self-interests and normative aspirations are inherently intertwined, and that norms and values most often run in parallel. This parallelism underscores the multifaceted nature of EU cybersecurity governance, where normative considerations inform and shape strategic objectives. Examples of this are international cooperation that can be considered both a norm and an

interest of the EU, as well as the interest in data privacy that overlaps with the protection of the Rule of Law, fundamental rights, and freedoms. Overall, the EU presents a united and coherent front in combating cyber threats and enhancing cybersecurity. One of the key strengths observed in the EU's cybersecurity policy efforts is its coherence and unity in addressing cyber threats. Despite variations in priorities and approaches among Member States, the EU presents a united front in promoting adherence to international law and common standards. While there are differences in focus in dialogues with different countries, there are no explicit signs of double standards compromising core values for economic gains. While the EU demonstrates a nuanced approach in its dialogues with different countries, particularly evident in its engagement with China, it's necessary to differentiate between this nuanced approach and outright double standards. The emphasis on economic cooperation over explicit cybersecurity concerns in dialogues with China may reflect the complex nature of EU-China relations with a delicate balance between economic interests and cybersecurity. This nuanced approach does not necessarily imply a compromise of core values but highlights the multifaceted nature of the EU's external engagements.

While normative considerations are present in the EU's cybersecurity discourse they are often intertwined with self-interests and pragmatic concerns, aligning more with an understanding of the EU as a market power. The EU's substantial market size not only shapes its internal regulatory standards but also enables it to project influence externally. Just as the EU leverages its market size to externalize economic and social policies in other domains, it also utilizes it in cybersecurity policy. For instance, the EU's emphasis on promoting economic stability and ensuring market access in cybersecurity dialogues reflects its recognition of the economic dimension of cybersecurity and its ability to shape international norms and standards through market incentives. As evident in the dataset, the EU's interests in protecting critical infrastructure, promoting economic stability, and ensuring market access are explicitly mentioned in various dialogues and strategies. They are therefore articulated as both an intention and demonstrated in practice. Economic considerations, innovation, and market competitiveness are significant interests reflected in EU's discussions and underscore its role as a market power. Dialogues with third countries occasionally prioritise economic cooperation over explicit cybersecurity concerns, indicating a focus on the economy rather than purely normative considerations.

This is, once again, the case in the dialogue with China and suggests an approach where economic interests are given precedence over other cybersecurity concerns.

As evidenced by the EU's references to the UN framework as well as the Budapest Convention, the EU actively promotes universally acknowledged norms and values. Commitment to the UN Framework for responsible state behaviour and promotion of the UN Cyber Programme of Action reflect a normative approach grounded in international consensus. To a certain extent, the EU emphasises cooperation and engagement with various stakeholders, including partner countries, international organisations, civil society, and the private sector. Efforts to involve diverse perspectives and expertise suggest a commitment to inclusiveness in policy formulation and decision-making. The EU demonstrates reflexivity by adapting its policies to specific contexts and needs, conducting impact assessments, and engaging in tailored capacity-building programs. Consideration of country-specific challenges, such as varying cybercrime investigative capacities, indicates a willingness to adjust policies based on evolving circumstances, all of which are indicative of normative process. By doing this, the EU ensures that its policies are responsive to evolving circumstances and effectively address the diverse cybersecurity landscape across different regions and countries. This is evident in several projects such as the iProceed2 where clear distinctions in needs are made between Montenegro, Serbia, and Türkiye (Council of Europe 2022a:2), as well as legislative assessments conducted within the Eastern European region (Council of Europe 2022b). Evidently, the EU reaffirms their ambition to involve the participation of the private sector and civil society and thus clearly demonstrates the multistakeholder model of internet governance that is part of what has been contested globally (Anagnostakis 2022:239-240).

However, its actions may also serve strategic interests such as maintaining influence in global cybersecurity governance. As briefly discussed in 5.2, the promotion of the Budapest Convention could be interpreted as a strategic move to counter alternative treaties supported by opposing countries such as Russia, China, and India, highlighting a pragmatic approach driven by the protection of interests. China argues for more state control in regulations of internet governance (Wood et al 2020) which would make this particularly important. The EU's emphasis on cooperation with stakeholders is noteworthy, yet there is a notable absence of explicit examples of engagement with civil

society organisations or representation of diverse perspectives in practice. This raises legitimate concerns regarding actual inclusiveness within the decision-making process. These tendencies could be indicative of Eurocentrism because it assumes that European norms are universally applicable and should be adopted by other countries without properly considering their unique cultural, social, and political contexts. Inclusiveness in cybersecurity governance would require more than just token representation. The EU need to engage in meaningful engagement and consultation with affected communities and stakeholders.

As previously stated, normative change is not as straightforward as the determining of normative intent and normative process. However, there are several instances where the EU has been able to induce normative change externally. The dialogue between the EU and Ukraine suggests that Ukraine is making efforts to align its cybersecurity policies and legislation with EU standards, indicating a convergence of norms between the EU and Ukraine. The emphasis on legislative reforms and alignment with international standards in the Southern Neighbourhood countries, such as Tunisia's accession to the Budapest Convention and the Data Protection Convention 108, indicates normative change influenced by EU initiatives. Projects in Southeast Europe, Türkiye, and the Eastern Partnership countries have led to tangible outcomes, such as the establishment of Computer Security Incident Response Teams (CIRTs)/Computer Emergency Response Teams (CERTs) and the adoption of advanced technology for cybersecurity measures. Moldova's digital transformation of public policy processes and alignment with the EU NIS Directive, as well as Georgia's adoption of the Law on Personal Data Protection, demonstrate normative change driven by EU efforts to build capacities and align with EU standards. However, it may be of value to view the EU's dialogues and projects in light of the global competition in cybersecurity governance. The EU's engagements may serve strategic objectives, such as extending influence, enhancing regional stability, or countering alternative cybersecurity governance proposed by opposing countries. As Kondrotas discusses (see 2.4) the EU tend to have difficulties in inducing normative change in states that stand far from the EU normatively. This thesis reaches similar conclusions as it is evident how the normative ties are proven to be stronger between the EU and countries that have expressed an ambition of accession to the EU. This is compared to the EU's cybersecurity relations with for example China and Korea where norms and values are not given the same attention.

6.1 Conclusion

The research has been conducted through a qualitative content analysis where EU strategy documents as well as external cybersecurity engagements have been analysed. This has been done by applying the theory of NPE by Ian Manners (2002), operationalized into three main categories by Niemann and de Wekker (2010) and applied through a deductively created codebook.

The conceptual framework of MPE argues that the EU does not need to be assigned a specific normative identity for us to understand the EU's power, but that focusing on its market reveals more about its identity and functioning (Damro 2012). While NPE highlights the EU's normative intent and commitment to promoting values in cybersecurity, this thesis concludes that MPE provides a complementary perspective by considering the interplay between normative goals and strategic market interests in shaping the EU's cybersecurity policy. As the evidence from the empirical findings shows, this thesis argues that the EU is a normative power to a large extent. Based on the normative theoretical framework applied to the 2020 EUCSS, the EU meets a preponderance of the requirements expected of a normative power. Where the EU falls short in Niemann and de Wekker's predefined categories of a normative power (see Table 1) is mainly regarding self-interests within normative intent and inclusiveness within the normative process. The occasional prioritising of interests can be explained by the logic of MPE rather than by NPE. The sometimes-lacking evidence of concrete involvement of civil society represents tendencies of a Euro-centric approach that Hettne & Söderbaum (2005) warn against. Based on the findings of this thesis alone, there is evidence of normative change induced by the EU. The analysis of normative change was however limited by factors previously discussed, such as language barriers which limited the choice of material to study. Whether the EU fully fulfils the requirements of normative change must therefore be left to further studies.

Both NPE and MPE offer valuable insights into the complex motivations and dynamics driving the EU's actions in the cyber domain. This thesis argues that the EU's engagement in cybersecurity cooperation with third countries can be viewed as serving both normative and economic interests. MPE acknowledges that the size of the Single market can work as an influence and attract third parties to align with EU standards. The 2020 EUCSS may

be influenced by considerations of market power and security competition, particularly in its interactions with other major powers like China where normative-driven arguments are lacking. All findings considered; however, this thesis argues that there is more evidence pointing towards normativity and that the theoretical frameworks by Ian Manners and Niemann & de Wekker shed light on this. The theoretical framework used in this thesis proved to be a helpful tool in the attempt to answer the research question. What has been consistently highlighted throughout this paper, however, is the shortcomings in detecting normative change in third countries. Just like Niemann & de Wekker argue, and as this thesis has acknowledged, normative change can only be approximated. This leaves a lot of room for further studies where a different, or an adjusted theoretical framework, may reach a more extensive result. It would be beneficial to study a set of countries in more depth to catch the national political and media discourse that Niemann and de Wekker propose but was not possible for this thesis due to the scope and language barriers. Likewise, to fully measure MPE's equivalent of normative change, externalisation, further research is needed. However, where the MPE mainly becomes important is in the realisation that the EU does not always act consistently in its external policies, as expressed by Damro (2012). In this sense, MPE serves as a framework with which EU foreign policy, including cybersecurity, can be analysed without being bound to perceptions of specific norms.

On a personal note, the research process allowed me to undergo significant growth as a researcher. I have not only deepened my knowledge of the EU and cybersecurity but also gotten valuable insights into the challenges of balancing theoretical framework with empirical evidence. Engaging with both NPE and MPE challenged me to think critically about the EU's actions and highlighted the complexity of the EU's role as both a normative and economic actor. In the aftermath, using NPE as operationalized by Niemann & de Wekker in this case, did not fully capture what was aimed for and what the framework has the potential to do. A qualitative case study studying only written material proved to be harder than anticipated, particularly in measuring the degree of normative impact. Just as previous scholars have debated, this may also be due to the need for NPE to be more flexible and nuanced (Jenichen 2022). It is these kinds of obstacles that highlight the long debate about what kind of power the EU possesses, and the challenges encountered in this study fuel this discussion.

As cybersecurity continues to be a growing field with significant implications for global security and governance, further research is needed to better understand the motivations and strategies of key actors such as the EU in shaping the cyber domain. Looking ahead, there are numerous areas for further exploration within the nexus of the EU and cybersecurity. A topic that this dissertation did not focus on is the intersection of cybersecurity and military strategy. This emerges as a compelling topic for future inquiry. As cyber threats increasingly blur the lines between traditional military domains and the digital realm, understanding the military aspect of cybersecurity becomes paramount. Further studies can thus delve into this evolving landscape to explore the implications for EU defence policies. As the debate on the EU's power dynamics persists, this research offers valuable insights into the EU's normative aspirations by asserting the EU's pivotal role as a normative power in shaping cybersecurity norms and behaviours. While there are certain aspects of the EU's actions that reflect market-oriented self-interests and a Eurocentric perspective, the overall evidence supports the conclusion that the EU embodies the characteristics of a genuine normative power in cybersecurity.

7. Bibliography

Empirical material

Breton, T. (2023a) A European Cyber Shield to step up our collective resilience | Opening of the International Cybersecurity Forum | Speech by Commissioner Thierry Breton. European Commission.

Breton, T. (2023b) Speech by Commissioner Breton on cybersecurity at the High-Level Conference on Cybersecurity in Republic of Korea.

Council of Europe (2021) CyberSouth - Cooperation on cybercrime in the Southern Neighbourhood Region. Project concept. https://rm.coe.int/3692-cybersouth-v13-extension-dec2021/1680a4d2a0 - Accessed: 2024-03-20.

Council of Europe (2022a) iProceeds-2. Project summary. https://rm.coe.int/2492-iproceeds-2-summary-v4/1680a6d081- Accessed: 2024-03-23.

Council of Europe (2022b) CyberEast - Action on Cybercrime for Cyber Resilience in the Eastern Partnership region (PMM 2088). Project summary and workplan. https://rm.coe.int/2088-cybereast-summary-and-workplan-december-2022/1680aa0773- Accessed: 2024-03-23.

Council of Europe (2023) CyberEast - Strategic Priorities for Cooperation on Cybercrime in the Eastern Partnership Region. https://rm.coe.int/2088-eap-strat-priorities-2023-v4-final-/1680ae1aa9 Accessed: 2024-04-02.

Council of the European Union (2022) Council conclusions on the development of the European Union's cyber posture - Council conclusions approved by the Council at its meeting on 23 May 2022.

Cybil Portal (2024a) Projects, iProceeds-2. https://cybilportal.org/projects/iproceeds-2/ Accessed: 2024-03-23.

European Commission (2020b) Joint communication to the European Parliament and the Council - The EUs cybersecurity strategy for the digital decade.

European Commission (2023a) Enhanced EU-Ukraine cooperation in Cybersecurity.

European Commission (2023b) 9th EU-US Cyber Dialogue in Brussels - press statement.

European Commission (2023c) Commission and China hold second High-level Digital Dialogue.

European External Action Service (2022) Ukraine and EU held the second round of the UA- EU Cybersecurity Dialogue. https://www.eeas.europa.eu/eeas/ukraine-and-eu-held-second-round-ua-eu-cybersecurity-dialogue_en Accessed: 2024-04-11.

European Union Agency for Cybersecurity (2021) International Strategy of the EU Agency for Cybersecurity.

EU4Digital (2023) EU supports new Moldova e-Monitoring system for policy implementation reform. https://eufordigital.eu/eu-supports-new-moldova-e-monitoring-system-for-policy-implementation-reform/ Accessed: 2024-04-18.

EU4Digital (2024a) Republic of Moldova approves draft law to strengthen cybersecurity. https://eufordigital.eu/republic-of-moldova-approves-draft-law-to-strengthen-cybersecurity/ Accessed: 2024-04-18.

EU4Digital (2024b) New data protection law taking effect in Georgia. https://eufordigital.eu/new-data-protection-law-taking-effect-in-georgia/ Accessed: 2024-04-18.

Literature:

Anagnostakis, D. (2022) "The External Face of the EU's Cybersecurity Policies: Promoting Good Cybersecurity Governance Abroad?" Cham: Springer International Publishing.

Bendiek, A. (2018) "The EU as a Force for Peace in International Cyber Diplomacy", German Institute for International and Security Affairs.

Bicchi, F. (2006) '"Our size fits all": normative power Europe and the Mediterranean', Journal of European Public Policy, 13(2), pp. 286–303.

Bryman, A. (2012) Social Research Methods, 4th edn. Oxford University Press.

Bull, H. (1982) "Civilian Power Europe: A Contradiction in Terms?", Journal of Common Market Studies 12(2): 149-6.

Carr, E. H. (1962) "The Twenty Years' Crisis 1919-1939: An Introduction to the Study of International Relations" 2nd edn, London: Macmillan.

Carrapico, H. and Barrinha, A. (2017) "The EU as a Coherent (Cyber)Security Actor", Journal of Common Market Studies, 55(6), pp. 1254–1272.

Carver, J. (2023) "More bark than bite? European digital sovereignty discourse and changes to the European Union's external relations policy", JOURNAL OF EUROPEAN PUBLIC POLICY [Preprint].

Collett, R. (2021) “Understanding cybersecurity capacity building and its relationship to norms and confidence building measures”, Journal of Cyber Policy, 6(3), pp. 298–317.

Council of Europe (2001) Convention on Cybercrime. https://rm.coe.int/1680081561 Accessed: 2024-02-12.

Council of the European Union (2015) Council Conclusions on Cyber Diplomacy, 6122/15, Brussels, 11 February.

Council of the European Union (2019) Council of the EU, Narrative Paper on an open, free, stable, and secure cyberspace in the context of international security´, 9764/1/19 REV 1, Brussels, 5 June 2019, p. 2.

Cybil Portal (2024b) The Knowledge Portal for Cyber Capacity Building. https://cybilportal.org/ Accessed: 2024-03-14.

Damro, C. (2012) “Market power Europe”, Journal of European Public Policy, 19(5), 682–699.

Damro, C. (2015) “Market power Europe: exploring a dynamic conceptual framework”, Journal of European Public Policy, 22(9), 1336–1354.

Diez, T (2005) ‘Constructing the Self and Changing Others: Reconsidering “normative power Europe”, Millennium, 33 (3), 613–36.

Diez, T. and Pace, M. (2007) ‘Normative Power Europe and Conflict Transformation”.

Duchêne., F (1972) ‘Europe’s Role in World Peace’, London: Fontana.

Duchene, F (1973) “The European Community and the uncertainties of interdependence. In: Kohnstamm M, Hager W (eds) A nations writ large? Foreign policy problems before the European Community”, MacMillan, London.

Duchêne, F. (1994) “Jean Monnet. The First Statesman of Interdependence”, New York And London: Norton.

Drisko, J. (2013). “Standards for qualitative studies and reports”. In R. Fortune, W. Reid, & R. Miller (Eds.), Qualitative research in social work (2nd ed., pp. 3–34). New York: Columbia University Press.

Drisko, J.W. (2016) “Content analysis”. Edited by T. Maschi. Oxford University Press (Pocket guides to social work research methods).

European Commission (2013) Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Cybersecurity Strategy for the European Union - An Open, Safe and Secure Cyberspace.

European Commission (2017) Joint communication to the European Parliament and the Council - Resilience, Deterrence and Defence: Building strong cybersecurity for the EU.

European Commission (2020a) New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391 Accessed: 2024-02-25.

European Commission (2024) Shaping Europe's Digital Future - Cybersecurity Policies. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies#ecl-inpage-kmq7bt98 Accessed: 2024-02-29.

EU CyberNet (2018) "Operational Guidance: Guide to the EU's International Cooperation on Cyber Capacity Building".

EU CyberNet (2024a) "About project"´.

Galtung, Johan (1973) "The European Community: a Superpower in the Making", Allen and Unwin: 1973.

Geddes, B. (2003) 'Big Questions, Little Answers, How the Questions You Choose Affect the Answers You Get', in Paradigms and Sand Castles (Ann Arbor, MI: Michigan University Press).

Halperin, S & Heath, O. (2020)´Political Research: Methods and Practical Skills´3rd edn. Oxford University Press.

Haroche, P. (2022). A'geopolitical commission': Supranationalism meets global Power competition. JCMS: Journal of Common Market Studies,61(4), 970–987.

Hettne, B. and Söderbaum, F. (2005) 'Civilian Power of Soft Imperialism? The EU as a Global Actor and the Role of Interregionalism', European Foreign Affairs Review, 10 (4), 535–52.

Hay, C. (2002)´Political Analysis: A Critical Introduction´. Palgrave.

Holsti, O. (1969) "Content analysis for the social sciences and humanities", Reading, MA: Addison-Wesley.

Hyde-Price, A. (2006) 'Normative" Power Europe: A Realist Critique', Journal of European Public Policy, 13 (2), 217–34.

Izycki, E., van Niekerk, B. and Ramluckan, T. (2023) 'Cyber Diplomacy: NATO/EU Engaging with the Global South', 2023 15th International Conference on Cyber Conflict: Meeting Reality (CyCon), Cyber Conflict: Meeting Reality (CyCon), 2023 15th International Conference on, pp. 417–435.

Jenichen, A. (2022) ‘The Politics of Normative Power Europe: Norm Entrepreneurs and Contestation in the Making of EU External Human Rights Policy’, Journal of Common Market Studies, 60(5), pp. 1299–1315.

Kasper. A. (2020) “EU cybersecurity governance – stakeholders and normative intentions towards integration”. In M. Harwood, S. Moncada, R. Pace, (Eds.), The future of the European Union: Demisting the Debate (pp. 166-185). Msida: Institute for European Studies.

Kim, M. and Choi, J. (2020) ‘What kind of power is the EU? The EU’s policies toward North Korea’s WMD programs and the debate about the EU’s role in the security arena’, Asia Europe Journal: Studies on Common Policy Challenges, 18(1), pp. 1–16.

Kondrotas, L. (2021) ‘European Union policy and the use of the normative power regarding cybersecurity’, Análisis Jurídico - Político, 4(7).

Krippendorff, K. (2018) “Content analysis. an introduction to its methodology” Fourth Edition, SAGE.

Manners, I. (2002) ‘Normative Power Europe: A Contradiction in Terms’, Journal of Common Market Studies, 40(2), pp. 235–258.

Manners, I. (2008) ‘The Normative Ethics of the European Union’, International Affairs, 84 (1), 45–60.

Maull H (1990) “Germany and Japan: the new civilian powers”, Foreign Aff 69(5):91–106.

Mayring, P. (2000) “Qualitative content analysis”. Forum Qualitative Sozialforschung/Forum: Qualitative Social Research, 1(2).

Niemann, A. and de Wekker, T. (2010) ‘Normative power Europe? EU relations with Moldova’, European Integration Online Papers, 14(1), pp. 1–41.

Noutcheva, G. (2009) ‘Fake, partial and imposed compliance: The limits of the EU’s normative power in the Western Balkans’, Journal of European Public Policy, 16(7), pp. 1065-1084–1084.

Orbie, J. (2006) ‘Civilian Power Europe: Review of the Original and Current Debates’, Cooperation and Conflict, 41(1), pp. 123–128.

Pâris, C. (2021) “Guardian of the Galaxy? Assessing the European Union’s International Actorness in Cyberspace”, College of Europe.

Pawlak, P. (2016) ‘Capacity Building in Cyberspace as an Instrument of Foreign Policy’, Global Policy, 7(1), pp. 83-92–92.

Pawlak, P. and Barmpaliou, P.-N. (2017) ‘Politics of cybersecurity capacity building: conundrum and opportunity’, Journal of Cyber Policy, 2(1), pp. 123–144.

Puetter, U. and Wiener, A. (2007) 'Accommodating Normative Divergence in European Foreign Policy Co-Ordination: The Example of the Iraq Crisis', Journal of Common Market Studies, 45(5), pp. 1065–1088.

Renard, T. (2018) 'EU cyber partnerships: assessing the EU strategic partnerships with third countries in the cyber domain', European Politics & Society, 19(3), pp. 321–337.

Schreier, M. (2012) "Qualitative content analysis in practice", Thousand Oaks, CA: Sage.

Sjursen H (2006a) The EU as a "normative" power: how can this be? J Eur Publ Policy 13(2):235–251.

Sjursen, H. (2006b) 'What Kind of Power?', Journal of European Public Policy, 13 (2), 16981.

Sliwinski, K.F. (2014) 'Moving beyond the European Union's Weakness as a Cyber-Security Agent', Contemporary Security Policy, 35(3), pp. 468-486–486.

Twitchett, K (ed) (1976) "Europe and the world: the external relations of the common market", Martin's Press, New York.

Weber, R. (1990) "Basic content analysis" (2nd ed.), Thousand Oaks, CA: Sage.

Whitman, R.G. (2011) "Normative power Europe. empirical and theoretical perspectives", Palgrave Macmillan (Palgrave studies in European Union politics).

Wood, S., Hoffmann, S., McFadden, M., Kaur, A., Wongsaroj, S., Schoentgen, A., Forsyth, G., and Wilkinson L. (2020). Digital sovereignty: The overlap and conflict between states, enterprises and citizens.

Youngs, R. (2004) 'Normative Dynamics and Strategic Interests in the EU's External Identity', Journal of Common Market Studies, 42 (2), 415–35.