Universiteit Leiden

THE EUROPEAN UNION’S GLOBAL AMBITION AND CYBERSPACE

Assessing the coherence between the EU’s external cybersecurity strategy and its willingness to become more active at the international level

Word count (including footnotes and bibliography): 14,970

Mattia Da Re
S2725207
m.r.da.re@umail.leidenuniv.nl

By submitting this, I certify that:

- ✓ this work has been drafted by me without any assistance from others (not applicable to group work);
- ✓ I have not discussed, shared, or copied assessment work from/with other students;
- ✓ I have not used sources that are not explicitly allowed by the course instructors and I have clearly referenced all sources (either from a printed source, internet or any other source) used in the work in accordance with the course requirements and the indications of the course instructors;
- ✓ this work has not been previously used for other courses in the program, unless explicitly allowed by the instructors.

I understand that any false claim in respect of this work will result in disciplinary action in accordance with university regulations and the program regulations, and that any false claim will be reported to the Board of Examiners. Disciplinary measures can result in exclusion from the course and/or the program, and in a permanent endorsement on my diploma.

I understand that my work may be checked for plagiarism, by the use of plagiarism detection software as well as through other measures taken by the university to prevent and check on fraud and plagiarism.

I understand and endorse the significance of the prevention of fraud and I acknowledge that in case of (gross) fraud the program could declare the exam invalid, which may have consequences for all students.

Table of Contents

Introduction

"Cyber-attacks threaten our lives and rights."[1] That is what Josep Borrell, the head of the European Union's (EU) diplomacy, declared after the EU released its new *Cybersecurity Strategy* on December 16th, 2020.[2] This statement demonstrates well the fear existing around misuses of cyberspace and Information and Communication Technologies (ICTs) since the beginning of the 21st century. To mitigate this threat, states and other actors of the international system have decided to take some actions, notably by publishing their own cybersecurity strategy.

The EU is no exception to the rule. Indeed, the EU published its first *Cybersecurity Strategy* in 2013.[3] In the beginning, the EU's policy was more focused on the internal dimension of its cybersecurity - the EU's own institutions' as well as member states' cyber technologies, internal laws, cyber crime inside the EU, etc. However, the external dimension - the interactions with other states, international organizations, multinational companies, etc. - of the EU's cybersecurity strategy also began to develop over the years. In parallel, the EU has formulated its ambition to be more active externally. In that regard, the organization has published its first *Security Strategy* in 2003[4] and has reiterated their ambition more concretely in 2016 with the publication of the *European Global Security Strategy* (EUGS).[5]

In light of these two recent developments, this thesis aims at exploring the relationship between the EU's formulated ambition to be more active at the international level and the EU's external cybersecurity strategy. In order to do that, the thesis will answer the following research question: "*How coherent is the European Union's external cybersecurity strategy with the EU's willingness to become more active at the international level ?*" More precisely, the thesis will assess whether the EU's external cybersecurity strategy corresponds to the key principles and helps fulfill the objectives set out by the EUGS for the EU to become more active externally.

The objective of this thesis is two-fold: scholarly and societal. On one hand, it intends to fill the gap existing in the literature around the EU's external cybersecurity strategy and its relationship with the EU's ambition to be more active on the global level. It also encourages further research on the topic. On the other hand, it offers EU policymakers an assessment of the

1[1] Borrell, Josep, "Make cyberspace a safer place," HR/VP Blog Post, December 17, 2020.

[2] European Commission and High Representative of the EU for Foreign Affairs and Security Policy, *The EU's Cybersecurity Strategy for the Digital Decade* (Brussels: European Union, December 16, 2020).

[3] European Commission and High Representative of the EU for Foreign Affairs and Security Policy, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* (Brussels: EU, February 7, 2013).

[4] Council of the EU, *European Security Strategy. A Secure Europe in a Better World* (Brussels: EU, 2003).

[5] European External Action Service (EEAS), *Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the EU's Foreign and Security Policy* (Brussels: EU, June 2016).

EU’s external cybersecurity strategy and provides them the opportunity to adjust and improve it, if needed. As mentioned earlier, cybersecurity is already a key area of action and signs suggest that this trend will increase in the future. It is therefore important for the EU to formulate the best strategy possible.

This thesis is organized as follows. The first chapter is dedicated to the literature review of the topic of the EU’s external cybersecurity strategy. The second chapter provides the methodology at the basis of this thesis. The third chapter intends to develop the theoretical framework upon which this thesis is constructed: the EU’s willingness to become more active at the international level. The fourth chapter is devoted to the data analysis part of the thesis and is divided into two subsections. One describes the main lines of the EU’s external cybersecurity strategy. The other assesses the coherence between the principles and guidelines set out in the theoretical framework and the EU’s external cybersecurity strategy. Finally, the conclusion summarizes the findings of the thesis and provides an answer to the research question.

Chapter 1 - Literature review

This chapter is dedicated to the literature review on the topic of the external dimension of the EU's cybersecurity strategy. The chapter's objective is two-fold. On one hand, it situates the research question in the already existing literature. On the other, it exposes the gaps existing in the literature that this paper intends to fill, and it, therefore, demonstrates this paper's relevance and novelty.

The literature focusing on EU cybersecurity is relatively seldom developed and most of the scientific pieces written on the topic are very recent. Indeed, the majority of the contributions to the scholarship were written after 2010. The two main reasons for this are, firstly, the fact that cyberspace security is a recent phenomenon, and secondly, the fact that EU policymakers have only begun to approach this issue seriously in the last couple of decades.

In the literature, there is a consensus around the fact that, when it comes to the European Union, the internal dimension of its cybersecurity strategy is much more developed than the external dimension. However, scholars present different arguments to explain this phenomenon. For instance, Sliwinski and Ivan both state that it is mostly the lack of shared conceptual definition over cyber issues and the intergovernmental logic that guides the EU's external policies that prevent it from having a more concrete and ambitious external cybersecurity strategy.[6] Bendiek agrees with their arguments and adds that cyberspace's specific characteristics can also explain this claim.[7] Because most policies taken have been about the internal dimension of EU cybersecurity, the scholarship has also been mostly focusing on this aspect.

Nevertheless, in recent years we have seen developments in the EU's external cybersecurity strategy. Scholars have advanced different arguments to explain the recent developments in this field. The most cited explanation is the increasing number, and sometimes complexity of cyber attacks, making the EU more afraid of the threats posed by cyberspace. Carrapico and Barrinha, Moret and Pawlak, and Renard have also posited that this fear is decoupled if we consider the increasing pervasiveness of cyberspace technologies as well as the almost-absolute reliance of European societies on technologies.[8] Moreover, Moret and

[6] Ivan, Paul, "Responding to cyberattacks: Prospects for the EU Cyber Diplomacy Toolbox," European Policy Centre, Discussion Paper, March 18, 2019, 7 ; Sliwinski, Krzysztof Feliks, "Moving beyond the European Union's Weakness as a Cyber-Security Agent," *Contemporary Security Policy* 35, no. 3 (2014), 479-480.

[7] Bendiek, Annegret, "European Cyber Security Policy," Stiftung Wissenschaft und Politik, Research Paper 13, October 2012, 19.

[8] Carrapico, Helena, and André Barrinha, "The EU as a Coherent (Cyber)Security Actor?," *Journal of Common Market Studies* 53, no. 6 (2017), 1255 ; Moret, Erica, and Patryk Pawlak, "The EU Cyber Diplomacy Toolbox : towards a cyber sanctions regime?," European Union Institute for Security Studies, Brief 24, July 2017, 1 ; Renard,

Pawlak have stated that the absence of "norms of responsible state behavior and international law in cyberspace" has made the EU aware that its engagement in this field was required.[9]

As it can be observed, these explanations focus on structural elements to justify the EU's actions. However, on their part, Odermatt, Renard, and Calleri have dared to claim that the recent developments in the external dimension of the EU cybersecurity strategy must also be linked with the EU as an actor of international relations, and more precisely with its willingness of the EU to become more active on the global arena. Unfortunately, only Calleri and Odermatt expand further on this specific link.[10]

In his piece, Odermatt describes the multiple ways in which the EU operates its cyber diplomacy. According to him, it could allow the EU to "be a leader in developing legal norms that apply to cyberspace" and help the EU to be more powerful on the global stage. However, Odermatt states that the EU lacks a "comprehensive framework that would allow the EU to play such a role".[11]

In her article, Calleri explores the efficiency and usefulness of the EU's approach to cyber diplomacy for becoming a global actor in cyberspace. Amongst her conclusions, Calleri states notably that there is a gap between the EU's expectations and the EU's capabilities in the cyber domain, and that "cyber diplomacy constitutes an effective tool for cyber-deterrence" as it increases the eventual costs of an attack.[12] Although it only focuses on some aspects of the EU's cybersecurity strategy, Calleri and Odermatt's articles has the merit of being the first scientific contributions to explore the link between EU's cybersecurity and itd ambition of being more active externally.

In 2014, Renard had already concluded that cyber diplomacy[13] is the primary framework for characterizing the EU's external cybersecurity strategy.[14] Other scholars have then joined Renard's opinion and arguments because further policies and documents adopted by the EU acknowledge cyber diplomacy as the primary framework for the EU's external actions regarding

Thomas, "The rise of cyber-diplomacy: the EU, its strategic partners and cyber-security," European Strategic Partnerships Observatory, Working Paper 7, June 2014, 7.

[9] Moret and Pawlak, "The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime?," 1.

[10] Calleri, Martina, "The European Union as a Global Actor in Cyberspace: Can the Cyber Sanctions Regime Effectively Deter Cyber-Threats?," *Romanian Cyber Security Journal* 2, no. 2 (Fall 2020), 3-9 ; Odermatt, Jed, "The European Union as a cybersecurity actor," chap. 17 in *Research Handbook on the EU's Common Foreign and Security Policy*, ed. by Steven Blockmans and Panos Koutrakos (Cheltenham, UK: Edward Elgar, 2018), 370 ; Renard, Thomas, "EU cyber partnerships: assessing the EU strategic partnerships with third countries in the cyber domain," *European Politics and Society* 19, no. 3 (2018), 322.

[11] Odermatt, "The European Union as a cybersecurity actor," 372.

[12] Calleri, "The European Union as a Global Actor in Cyberspace: Can the Cyber Sanctions Regime Effectively Deter Cyber-Threats?,"8.

[13] In brief, cyber diplomacy consists in using the means of diplomacy to tackle issues related to cyberspace.

[14] Renard, "The rise of cyber-diplomacy : the EU, its strategic partners and cyber security."

its cybersecurity.[15] More recently, on the 16th December 2020, the EU has published a new *Cybersecurity Strategy*. However, given the fact that this new strategy was published very recently, scholars have not had the time to analyse it.[16]

From the literature review, it can be concluded that the external dimension of the EU's cybersecurity strategy is very recent. This is true both at the policymakers- and scholars-level. Even though the recent developments have encouraged scholars to claim that cyber diplomacy is the primary framework to consider the EU's actions in the international realm concerning cybersecurity, there are still some unexplored issues concerning the EU's cybersecurity. The primary noticeable gap is the absence of a study exploring the link between the EU's external cybersecurity strategy and the EU's willingness to become more active at the international level. Even though Renard, Odermatt, and Calleri have posited that such a link exists, the relationship between these two elements has been seldom explored.

This thesis is thus dedicated to addressing the gap in the literature around the relationship between the EU's external cybersecurity strategy and the EU's willingness to be more active externally. More precisely, it intends to answer the following research question: "*How coherent is the European Union's external cybersecurity strategy with the EU's willingness to become more active at the international level ?*" The next chapter will explain the methodology applied in this thesis to answer the research question.

[15] Bendiek, Annegret, "The EU as a Force for Peace in International Cyber Diplomacy," Stiftung Wissenschaft und Politik, SWP Comment 19, April 2018 ; Carrapico and Barrinha, "The EU as a Coherent (Cyber)Security Actor?," 1266 ; "Moret and Pawlak, "The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime?."

[16] European Commission and High Representative of the EU for Foreign Affairs and Security Policy, *The EU's Cybersecurity Strategy for the Digital Decade.*

Chapter 2 - Methodology

A) Research Design

The research design has been constructed in order to answer the research question. It wishes to explore one aspect of the connections between two variables. Firstly, there is the EU's willingness to become more active at the international level. Secondly, there is the EU's external cybersecurity strategy.

The first part of the thesis is dedicated to exploring the EU's willingness to play a more active role at the international level. This will be done in the theoretical framework of the thesis. In this section, the guiding principles of the EU's strategy to become more active internationally will be presented. Firstly, this will give indications on what to look for when investigating the EU's external cybersecurity strategy. Secondly, this will provide the framework of analysis for considering whether the EU's external cybersecurity strategy is coherent with the EU's objectives and guiding principles regarding its willingness to become a global security actor.

The second part of the thesis is concerned with exploring the EU's external cybersecurity strategy. This will be done in the data analysis section of the thesis. One subsection is dedicated to frame and explaining what the EU's external cybersecurity strategy is. This subsection will present the key documents and general principles of the EU's external cybersecurity strategy. The second subsection is concerned with assessing the EU's external cybersecurity strategy in relation to the theoretical framework of this paper. The subsection's organization is based on the framework of analysis presented in the theoretical framework. It will assess the coherence between the EU's objectives and guiding principles presented in the theoretical framework and the EU's external cybersecurity strategy. More specifically, the coherence will be assessed by comparing the guiding principles and areas of actions that the EU recommends to fulfill its objective of becoming more active at the international level with the characteristics of the EU's external cybersecurity strategy. In turn, this will answer the research question at the basis of this thesis.

B) Research Methods

a) Data collection and data selection

The theoretical framework is constructed based on one specific document: the *European Union Global Strategy* released in June 2016.[17] The rationale for using the EUGS as the basis for the theoretical framework is that the document was written to provide the EU a strategy for guiding the EU's future external actions. Moreover, the EUGS is still applicable at the time of writing this thesis. As such, it provides the main guidelines, priorities, and principles to analyse and to assess the EU's external actions in general as well as those concerning cybersecurity.

Because the EUGS was published in 2016, it has already been thoroughly analyzed by the scholarship. This section is thus based on both a content analysis of the EUGS and a content analysis of the already existing literature around it. Moreover, to be as most context-relevant as possible, the section draws also on more recent official documents and statements made by current High Representative Josep Borrell and the President of the European Commission Ursula von der Leyen, who both took office in December 2019, that might highlight more recent principles and guidelines about the EU's external actions.[18]

The choice to use EU official documents to construct the theoretical framework is primarily motivated by the willingness to explain and describe what the EU's objectives are as presented in its organization's documents, and assess the coherence between the EU's own objectives and its external cybersecurity strategy. This approach is preferred to the one that seeks to analyse the EU's external cybersecurity strategy with other theoretical frameworks that do not entirely fit the context of the EU.

The second section of this paper is based on the analysis of the EU official documents related to the topic of cybersecurity. The timeframe for the data collection is 2013 to 2020. The year 2013 corresponds to the publication date of the first EU *Cybersecurity Strategy* document: the EUCSS.[19] The collection of these data was made by researching the database of the European Union website. The choice of basing this section on multiple documents rather than to focus on one, for instance, the more recent *Cybersecurity Strategy* of 2020[20], is justified by the fact that it allows seeing the changes in the EU cybersecurity strategy over time. Moreover, it offers more details and information about the topic and allows observing which characteristics prevail in the EU's external cybersecurity strategy.

b) Data analysis

[17] EEAS, *Shared Vision, Common Action: A Stronger Europe.*

[18] See Bibliography for full references.

[19] European Commission and High Representative of the EU for Foreign Affairs and Security Policy, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*.

[20] European Commission and High Representative of the EU for Foreign Affairs and Security Policy*, The EU's Cybersecurity Strategy for the Digital Decade*.

The data collected are composed mainly of documents. These can go from official documents and statements made by EU policymakers to secondary literature written on the topic to newspaper articles. The method for analysing these documents will be based on content analysis. This method consists of interpreting the documents selected to "elicit meaning, gain understanding, and develop empirical knowledge."[21] To do this, the data contained in the documents are regrouped into categories related to the research question allowing themes and patterns to appear in the documents selected. Therefore selecting the right documents is crucial. The major factor to select documents should be their relation to the topic of the study. A good document is one that contains many evidence or links to the purpose of the thesis.[22] To avoid bias and unreliabilities in the document analysed, the researcher should seek to select multiple documents to corroborate the findings.[23]

There are many advantages to using content analysis. First of all, it is less time consuming because the documents are already available. The researchers must only select the one he wishes to analyse. Moreover, many documents are available and easy-to-access. This is especially true for an organization like the European Union which produces many bureaucratic documents. Furthermore, the documents analysed are not produced by the researchers. They are thus not influenced by its bias(es). However, the documents are context-dependent. This means that they are influenced by the producers, the period, and the objectives of the producers. The researchers must take into account all of these elements. This is not the only flaw of content analysis. Another disadvantage is that the documents can not cover everything. The researcher's scope will therefore be limited if he only uses content analysis for his study. One way to get around this problem is to triangulate the evidence found in the documents with other data like interviews.[24] The lack of data triangulation is one of the flaws of this thesis. Indeed, the data analysis draws almost exclusively on documents published by the European Union.

c) Other limits

[21] Bowen, Glenn, "Document Analysis as a Qualitative Research Method," *Qualitative Research Journal* 9, no. 2 (2009), 27.

[22] Bowen, "Document Analysis as a Qualitative Research Method," 32 ; Julien, Heidi, "Content Analysis," in *The SAGE Encyclopedia of Qualitative Research Methods,* ed. by Lisa M. Given (Thousand Oaks, CA: SAGE Publications, 2012), 121.

[23] Bowen, "Document Analysis as a Qualitative Research Method," 28.

[24] Bowen, "Document Analysis as a Qualitative Research Method," 31-32 : Heidi, "Content Analysis," 122 ; Lamont, Christopher, "Qualitative Methods in International Relations," chap. 5 in *Research Methods in International Relations* (Thousand Oaks, CA: SAGE Publications, 2015), 82-83.

Besides the downsides of using content analysis explained here above, the major limitation of this thesis is that it only focuses on the EU strategy as described in the official documents. It lacks the analysis of the concrete actions to implement the EU strategy. The fact that this thesis does not cover this aspect of the EU external cybersecurity engagement is justified by the limited word count allowed for the realisation of this paper. The choice to focus only on the strategy as presented in the document responds however to the need to fill a gap in the literature and provides a first step before engaging in the EU's external actions in cybersecurity.

Another limitation is due to the special period during which this thesis was written. Indeed, the COVID-19 outbreak has severely limited the means to gather data, most notably the resources available in libraries and the conduct of interviews. That is the primary reason why this thesis is almost entirely based on data collected through online databases.

After having explained the methodology, the next chapter is dedicated to explaining the theoretical framework used in this thesis.

Chapter 3 - Theoretical framework: the EU's willingness to become more active externally

In this section, the theoretical framework for the thesis will be presented. It concerns the EU's willingness to be more active at the international level.

The European Union is an international actor. This claim is acknowledged since nearly the beginnings of European integration.[25] What has been more debated between scholars as well as policymakers is the exact role that the EU plays - or should play - at the international level. However, since a couple of decades, observers have witnessed the EU's ambitions to have a more active role on the global stage. This has manifested multiple times since the 2000s.[26] For instance, in the introduction of the first *Security Strategy* of the EU, the *European Security Strategy* (ESS) published in 2003, it is stated that "Europe should be ready to share in the responsibility for global security and in building a better world."[27]

The willingness to be more active was renewed when the second security strategy, the *European Union Global Strategy*, was released in June 2016.[28] This ambition is clear since the early pages of the document: "We need a stronger Europe. This is what our citizens deserve, this is what the wider world expects."[29] This ambition is also present in the von der Leyen Commission that took office in December 2019. Ursula von der Leyen and Josep Borrell have reiterated their wish for 'a stronger Europe in the world' several times. The President of the Commission has even declared that her Commission will be a geopolitical one.[30] However,

[25] Jorgensen, Knud-Erik, and Yonatan Schvartzman, "The EU as a Global Actor," chap. 1 in *The European Union as a Global Health Actor*, ed. by Thea Emmerling, Ilona Kickbush and Michaela Told (Singapore, World Scientific, 2016), 1.

[26] Council of the EU, *European Security Strategy. A Secure Europe in a Better World* ; Mälksoo, Maria. "From the ESS to the EU Global Strategy: external policy, internal purpose," *Contemporary Security Policy* 37, no. 3 (2016), 378-379 ; Renard, Thomas, "The European Union: A New Security Actor," Robert Schuman Centre for Advanced Studies, EUI Working Paper 45, April 2014, 10.

[27] Council of the EU, *European Security Strategy,* 3.

[28] Biscop, Sven, "Strategy," chap. 2 in *European Strategy in the 21st Century. New Future for Old Power* (London, UK: Routledge, 2018), 31 ; Dijkstra, Hylke, "Introduction: one-and-a-half cheers for the EU Global Strategy," *Contemporary Security Policy* 37, no. 3 (2016), 371 ; EEAS, *Shared Vision, Common Action: A Stronger Europe* ; Mälksoo, "From the ESS to the EU Global Strategy: external policy, internal purpose," 380 ; Smith, Karen E., "A European Union global strategy for a changing world?," *International Politics* 54 (2017), 510.

[29] EEAS, *Shared Vision, Common Action: A Stronger Europe*, 7.

[30] Borrell, Josep, "A stronger European Union within a better, greener and safer world - key principles that will be guiding my mandate," HR/VP Blog Post, December 1, 2019 ; European Commission, *The von der Leyen Commission: for a Union that strives for more* ; European Commission, *Speech by President-elect von der Leyen in the European Parliament Plenary on the occasion of the presentation of her College of Commissioners and their programme* (Strasbourg: European Union, November 27, 2019) ; von der Leyen, Ursula, *A Union that strives for more. My agenda for Europe: Political guidelines for the next European Commission 2019-2024* (Brussels: European Union, October 9, 2019).

merely stating its ambition to be more active is not sufficient. The EUGS also describes the principles and priorities that must guide the EU's actions.

When reading through the EUGS, some principles guiding the EU's actions stand out. One of which is the idea of principled pragmatism which is described as "a realistic assessment of the strategic environment [coupled with] an idealistic aspiration to advance a better world."[31] Principled pragmatism does not mean that the EU is abandoning its values. Rather, instead of wanting to engage in the world with actions solely based on its internal values, the EU recognizes that it has to assess what is realistically and pragmatically possible to achieve. This entails a case-by-case approach to engage in the world.[32] Biscop has described this idea as 'realpolitik with European characteristics'.[33] Here again, the new European Commission embraces these guidelines and argues that the EU's external actions must be guided by its values but also calls for more realism.[34] The values and rules that the EU promotes are based on the UN Charter and fundamental rights. These include "respect for and promotion of human rights, fundamental freedoms and the rule of law. They encompass justice, solidarity, equality, non-discrimination, pluralism, and respect for diversity."[35]

Another guiding principle advanced in the EUGS is the principle of state and societal resilience. Understood as "the ability of states and societies to reform, thus withstanding and recovering from internal and external crises"[36], resilience is intended to replace the norms-promotion and democracy-exportation agendas of the EU which was considered and proven unrealistic. Resilience-building allows for more flexible and tailored ways of cooperating with third countries, including more authoritarian regimes. According to the EUGS, a resilient state is well-governed, inclusive, and sustainable. Moreover, resilience is intended to bring more security to the European Union because non-resilient states are not stable and therefore can ultimately bring more instability into the world, which will impact the EU.[37]

This makes the link with another key feature of the EUGS: the emphasis put on the EU's citizens. With the EUGS, the European foreign policy is first-and-foremost dedicated to improving the well-being of Europeans. The EUGS recognizes the blurring frontier between

[31] EEAS, *Shared Vision, Common Action: A Stronger Europe,* 16.

[32] Biscop, "Strategy," 31-32 ; Giusti, Serena, "The European Union Global Strategy and the EU's Maieutic Role," *Journal of Common Market Studies* 58, no. 6 (2020), 1455 ; Smith, "A European Union global strategy for a changing world?," 510 ; Tereszkiewicz, Filip, "The European Union as a normal international actor: an analysis of the EU Global Strategy," *International Politics* 57, no. 1 (2020), 107-10 ; Tocci, Nathalie, "Resilience and the role of the European Union in the world," *Contemporary Security Policy* 41, no. 2 (2020), 179-180.

[33] Biscop, "Strategy," 31.

[34] Borrell, "A stronger European Union within a better, greener and safer world."

[35] EEAS, *Shared Vision, Common Action: A Stronger Europe*, 15.

[36] Ibid., 23.

[37] Tereszkiewicz, "The European Union as a normal international actor: an analysis of the EU Global Strategy," 109-110 ; "Tocci, "Resilience and the role of the European Union in the world," 177-182.

internal and external politics as its inherent objective is to increase its UE's citizens' prosperity and security.[38] Indeed, 'The Security of Our Union' corresponds to the first priority of the EUGS listed in the document.[39] This feature is also present in the von der Leyen Commission's priorities. European citizens' prosperity and security must be the objective of Europe's external actions.[40]

In order to better fulfill this objective, the EU has chosen to narrow their focus of action on their close neighbourhood to the South and East. Indeed, an unstable neighbourhood has more impact inside the borders of the EU. Accordingly, the EUGS states that the EU "will take responsibility foremost in Europe and its surrounding regions, while pursuing targeted engagement further afield."[41]

Another feature of the EUGS is the willingness to increase the EU's engagement in the world through inter-regionalism. The EUGS considers that "regions represent critical spaces of governance in a de-centred world."[42] As such, they represent the ideal partners for the EU on global issues. Therefore, the EU must promote and support efforts of regionalization in the world, whether it is an elite-led initiative or a bottom-up approach. Furthermore, the EUGS calls the EU's institutions to increase the means of cooperation with these regional systems.[43]

This is a part of a wider ambition present in the EUGS: promoting a rules-based multilateral order. Indeed, the EU recognizes that some issues cannot be managed and solved alone. Therefore, the EU calls for global governance based on multilateral decisions. The UN remains the framework under which these decisions ought to be taken.[44] As the EUGS mentions: "The EU will strive for a strong UN as the bedrock of the multilateral rules-based order, and develop globally coordinated responses with international and regional organisations, states and non-states actors."[45] The EU aims at increasing as well as deepening the multilateral order. To do so, the EU says that it will 'lead by example' in implementing the UN's decisions and propose initiatives.[46] Promoting a rules-based order based on multilateralism is also a significant feature of the current European Commission. At multiple

[38] Biscop, "Strategy," 32 ; Dijkstra, "Introduction: one-and-a-half cheers for the EU Global Strategy," 370 ; Mälksoo, "From the ESS to the EU Global Strategy: external policy, internal purpose," 380.

[39] EEAS, *Shared Vision, Common Action: A Stronger Europe*, 19.

[40] European Commission, *Speech by President-elect von der Leyen in the European Parliament Plenary on the occasion of the presentation of her College of Commissioners and their programme.*

[41] EEAS, *Shared Vision, Common Action: A Stronger Europe*, 18.

[42] EEAS, *Shared Vision, Common Action: A Stronger Europe*, 32.

[43] Biscop, "Strategy," 34 ; EEAS, *Shared Vision, Common Action: A Stronger Europe*, 32-39.

[44] Biscop, "Strategy," 32 ; 34-35 ; Tereszkiewicz, "The European Union as a normal international actor: an analysis of the EU Global Strategy," 102.

[45] EEAS, *Shared Vision, Common Action: A Stronger Europe*, 39.

[46] Ibid., 39-44.

times, von der Leyen and Borrell have claimed that the EU is and must remain 'a champion of multilateralism'.[47]

The EUGS also advocates a strong sense of unity in the EU. Accordingly, "[o]nly the combined weight of a true union has the potential to deliver security, prosperity and democracy to its citizens and make a positive difference in the world."[48] This 'unity' entails dialogues, cooperation, interoperability, a sense of consensus between EU Member states as well as EU institutions.[49] This call for unity is also advocated by the current European Commission.[50]

All of the guidelines presented above and in the EUGS relies mostly on soft power. Indeed, the importance of diplomacy is greatly highlighted in the EU document. Davis Cross even states that the document in itself is a diplomatic exercise because of the timing of its release, only several days after the Brexit vote.[51] This is not a surprise as diplomacy is the privileged tool for the EU's external actions.[52] However, in contrast to the ESS of 2003, the EUGS goes further and states that "soft power is not enough".[53] The EUGS suggests that the EU should use all the means at its disposal because "soft and hard power goes hand in hand".[54]

Furthermore, the EU must then increase its defence capacities in cooperation with each other and strive towards strategic autonomy, while still acknowledging NATO as the principal framework for most EU Member States.[55] The willingness to use every tool at the EU's disposal to advance its interests at the international level is also very present in the 2019-2024 European Commission's programme. Indeed, in the mission letter sent to Josep Borrell, Ursula von der Leyen urges him to "use our diplomatic and economic strength" and "ensure [that] our external financial instruments are used strategically, contribute to our wider political aims and enhance

[47] Borrell, "A stronger European Union within a better, greener and safer world" ; European Commission, *Speech by President-elect von der Leyen in the European Parliament Plenary on the occasion of the presentation of her College of Commissioners and their programme ;* von der Leyen, *A Union that strives for more.*

[48] EEAS, *Shared Vision, Common Action: A Stronger Europe,* 6.

[49] Novotná, Tereza, "The EU as a Global Actor: United We Stand, Divided We Fall," *Journal of Common Market Studies* 55 (September 2017), 178.

[50] Borrell, "A stronger European Union within a better, greener and safer world" ; von der Leyen, *A Union that strives for more.*

[51] Davis Cross, Mai'a K., "The EU Global Strategy and diplomacy," *Contemporary Security Policy* 37, no. 3 (2016), 402.

[52] Tereszkiewicz, "The European Union as a normal international actor: an analysis of the EU Global Strategy," 102.

[53] EEAS, *Shared Vision, Common Action: A Stronger Europe,* 44.

[54] Ibid., 4.

[55] EEAS, *Shared Vision, Common Action: A Stronger Europe,* 19-20 ; Dijkstra, "Introduction: one-and-a-half cheers for the EU Global Strategy," 371.

Europe's leadership and influence in the world."[56] Also, von der Leyen wants the EU to take "bold steps" towards a "genuine European Defence Union".[57]

In summary, the EUGS published in 2016 has posited the guidelines and principles for the EU's external strategy in order to become more active externally. These guidelines are still relevant today. This is proved by the statements of Ursula von der Leyen and Josep Borrell. These principles are: principled pragmatism; focusing on resilience-building instead of democracy-promotion; encouraging and fostering the unity between Member States and EU institutions; the emphasis put on European citizens' prosperity and security; the promotion of a multilateral rules-based order; encourage inter-regionalism cooperation; the focus on the 'close' neighbourhood; the renewed importance of diplomacy; the acknowledgement that 'soft and hard power go hand in hand', and; the ambition to increase Europe's strategic autonomy, most notably through defence spending.

These guidelines will be the framework upon which analysing and assessing the EU's external cybersecurity strategy which will be done in the next chapter.

[56] European Commission, *Mission letter to Josep Borrell, High Representative of the Union for Foreign Affairs and Security Policy/Vice-President of the European Commission.*

[57] Ibid.

Chapter 4 - Data analysis

I. Framing the EU's external cybersecurity strategy

In this section, the EU's external cybersecurity strategy will be framed. More specifically, the key documents published by the EU related to this domain will be presented to describe, without entering too much into the details, the EU's external cybersecurity strategy. This section serves as an introduction to the next section where the EU's external cybersecurity strategy's coherence with its ambition to be more active at the international level is assessed.

First of all, it is essential to note that the EU's cybersecurity strategy is still in development. This claim holds even more true concerning the external dimension. Indeed, the first key document published by the EU on cybersecurity is dated from February 2013, not so long ago. This document is the first EU *Cybersecurity Strategy*, the *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* (EUCSS).[58] It has been jointly adopted by the European Commission and the High Representative of the European Union for Foreign Affairs and Security Policy. This fact is significant because it links the EU's internal and external security.

The EUCSS lists the principles that should guide the EU's actions in the field of cybersecurity: the EU's core values apply as much in the digital as in the physical world; fundamental rights and freedoms must be protected; Internet access must be guaranteed to all; a democratic and efficient multi-stakeholder governance must be promoted; and, a shared responsibility between stakeholders is needed to ensure security in cyberspace.[59]

Even though the EUCSS is more concerned with the internal implications of cybersecurity, the third and fifth strategic priorities listed consist respectively in "developing cyberdefence policy and capabilities related to the CSDP" and "establishing a coherent international cyberspace policy for the EU and promoting core EU values".[60]

In November 2014, the Council of the EU adopted the *EU Cyber Defence Policy Framework*.[61] The objective of this document is "to provide a framework [...] to the cyber defence aspects of the EU Cybersecurity strategy."[62] Among other things, the document lists some priorities for the EU cyber defence. These focus mostly on the defence of the information

[58] European Commission and High Representative of the EU for Foreign Affairs and Security Policy, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*.

[59] Ibid., 3-4.

[60] Ibid., 4-5.

[61] Council of the EU, *EU Cyber Defence Policy Framework* (Brussels: EU, November 18, 2014).

[62] Ibid., 2.

and communication systems used by Member States and EU entities, for instance, protecting the communications between EU institutions. However, one of the priorities listed in the document is concerned with enhancing cooperation with international partners, notably NATO.

In 2018, the *EU Cyber Defence Policy* is updated to respond to changing security challenges and other transformations that have occurred since 2014.[63] The priorities do not change and the focus is still put on the defence of the information and communications systems used by Member States and EU institutions even though the sixth priority is concerned with enhancing cooperation with relevant international partners. However, the document is fairly longer, more detailed, and up-to-date.

In February 2015, the Council of the EU adopted the *Council Conclusions on Cyber Diplomacy*.[64] This document marks the official adoption of cyber diplomacy as the framework for the EU's external actions in cybersecurity. It states that the EU has to promote fundamental rights and EU values in international discussions about cyber issues. Also, the EU has to engage with third parties, whether public or private actors, in bilateral or multilateral ways.

Two years later, the Council of the European Union furthers the EU's efforts in cyber diplomacy by adopting the *Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities* in June 2017.[65] This document is to be completed with the *Implementing guidelines* published four months later.[66] These two documents form the 'Cyber Diplomacy Toolbox'. With these, the EU shows its determination to prevent and resolve international disputes in cyberspace through peaceful and diplomatic means as well as the measures that need to be taken to fulfill this two-fold objective. These are :

- preventive measures, including confidence-building measures, raising awareness on EU policies, and EU cyber capacity building in third countries,
- cooperative measures through EU-led political and thematic dialogues or démarches by the EU delegations,
- stability measures, including statements by the High Representative or Council Conclusions,
- restrictive measures, including sanctions like travel ban or freezing funds,
- and, possible EU support to Member States' lawful responses, including collective defense or assistance.[67]

[63] Council of the EU, *EU Cyber Defence Policy Framework (2018 update)*, (Brussels: EU, November 19, 2018).
[64] Council of the EU, *Council Conclusions on Cyber Diplomacy* (Brussels: EU, February 11, 2015).
[65] Council of the EU, *Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")* (Brussels: EU June 19, 2017).
[66] Council of the EU, *Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities* (Brussels: EU, October 9, 2017).
[67] Ibid., 6-14.

The document adds also that these measures can be implemented separately or jointly and that clear attribution is not required for these measures to be taken.

The *Cyber Diplomacy Toolbox* makes clear that the EU's external actions concerning cybersecurity are evolving from a reactive to a proactive approach that intends to deter malicious activities in cyberspace. Moreover, with these documents, the EU signals its intention to sanction the actors, whether it is a state, an individual, or an entity, that threaten the EU's security in cyberspace.

This is further elaborated in the *Council decision concerning restrictive measures against cyber-attacks threatening the Union or its Member States* published in May 2019.[68] This document clarifies the use of restrictive measures concerning cyber-attacks. It provides a conceptual framework and allows the EU to impose sanctions on persons or entities that are responsible for cyber-attacks or attempted cyber-attacks, or that provide financial, technical, or material support for such attacks, or that are involved in other ways. The sanctions include travel bans and the freezing of the funds and economic resources of these persons or entities. It marks the creation of a 'cyber sanction regime' for the EU. In July 2020, the EU has, for the first time, used these restrictive measures on six individuals and three entities that were involved in various cyber-attacks including 'WannaCry' and 'NotPetya'.[69]

Finally, in December 2020, the Commission and the High Representative jointly adopt the second *Cybersecurity Strategy* of the EU, *The EU's Cybersecurity for the Digital Decade.*[70] In this new strategy, increasing external actions is much more put forward than in the 2013 document as internal security is always linked with external efforts. Amongst other things, the 2020 strategy lists three areas of action for the EU, namely : (1) resilience, technological sovereignty and leadership ; (2) building operational capacity to prevent, deter and respond ; and, (3) advancing a global and open cyberspace.

Besides the advantage of giving contextual information about the EU's external cybersecurity strategy, this section clearly demonstrates the EU's increasing ambition to develop and expand its external cybersecurity strategy since 2013. Josep Borrell, the current head of EU diplomacy, has even declared that the new Cybersecurity Strategy of 2020 "puts

[68] Council of the EU, *Council decision concerning restrictive measures against cyber-attacks threatening the Union or its Member States* (Brussels: EU, May 14, 2019).

[69] Council of the EU, *Declaration by the High Representative Josep Borrell on behalf of the EU: European Union response to promote international security and stability in cyberspace* (Brussels: EU, July 30, 2020).

[70] European Commission and High Representative of the EU for Foreign Affairs and Security Policy, *The EU's Cybersecurity Strategy for the Digital Decade*.

forward a number of concrete proposals for a more decisive and ambitious external cyber policy."[71]

II. Assessing the coherence of the EU's external cybersecurity with the EU's willingness to become more active at the international level

In this section, the coherence between the objectives and guiding principles of the EU's willingness to become more active at the international level, described in the theoretical framework of this thesis, and its external cybersecurity strategy is assessed.

Importance of diplomacy

Diplomacy is the primary framework for the EU's external strategy toward cybersecurity. This practice is known as cyber diplomacy. Since 2013 and the first *Cybersecurity Strategy,* the EU has always privileged diplomacy to handle cyber issues and promote the EU's interests in cyberspace. For instance, 'Establish a coherent international cyberspace policy for the European Union and promote core EU values' is one of the five strategic priorities of actions listed in the EUCSS of 2013.[72] Moreover, The EU has always supported a multi-stakeholder model of governance for cyber issues. This is coherent with its willingness to address cyber issues with diplomacy because it entails dialogue and cooperation amongst the actors involved in cyberspace.

In 2015, the EU officially acknowledged the concept of 'cyber diplomacy' as the primary framework for their external actions concerning cyberspace. According to the *Council Conclusions on Cyber Diplomacy* released in February 2015, the EU supports an approach for cyber diplomacy that : (a) promotes and protects Human Rights and EU fundamental values ; (b) contributes to greater stability ; (c) promotes a multi-stakeholder model of governance ; (d) supports the idea that international laws apply as much in cyberspace as it does 'offline'.[73] Furthermore, the EU should engage with key partners. It concerns international organizations, states, NGOs, civil society, private companies in bilateral or multilateral fora.[74] The analysis of the documents published afterwards suggests that these principles still guide the EU's cyber diplomacy today.

[71] Borrell, "Make cyberspace a safe place."

[72] European Commission and High Representative of the EU for Foreign Affairs and Security Policy, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, 4-5.

[73] Council of the EU, *Council Conclusions on Cyber Diplomacy*, 4.

[74] Ibid., 11.

Since the release of this document, the EU has renewed and increased its interest in cyber diplomacy on several occasions in almost every document released concerning cybersecurity. The EU *Cyber Diplomacy Toolbox* of June and its *Implementing guidelines* of October 2017 are a good illustration of this claim.

In these two documents, the EU "reaffirms its commitment to the settlement of international disputes in cyberspace by peaceful means"[75] and decides on five types of measures to better respond, prevent and deter uses of cyberspace that go against EU interests and values. Three of these measures are exclusively of diplomatic nature. These consist of preventive measures such confidence-building measures to awareness-raising through dialogues and communications. There are also cooperative measures that enhance cooperation between the EU and other cyber actors. And finally, there are the stability measures such as statements or Council conclusions that can have signaling and condemning functions.[76] The EU has put these stability measures in application by issuing statements condemning cyber attacks.[77] For instance, in October 2018, a statement from the President of the European Council Donald Tusk, the President of the European Commission Jean-Claude Juncker and the High Representative Federica Mogherini was released condemning the Russian military intelligence service for a cyber attack on the Organisation for the Prohibition of Chemical Weapons.[78]

The *Cyber Diplomacy Toolbox* is thus a great indicator of the willingness to put cyber diplomacy as the center of the EU's external actions in cyberspace. However, with these documents, the EU goes further in this field. Before, cyber diplomacy was presented as a way to advance the EU's interests and values in cyberspace. The *Cyber Diplomacy Toolbox* indicates that cyber diplomacy can now be used to respond to and deter cyber threats in order to reinforce the EU's and its Member States' security.

In the new *Cybersecurity Strategy* of the EU just released in December 2020, cyber diplomacy's role is reinforced again. Indeed, the new *Cybersecurity Strategy* calls for a strengthening of the *Cyber Diplomacy Toolbox* as well as increasing the EU's engagement on

[75] Council of the EU, *Council Conclusions on a Framework for a Joint EU Diplomatic Responses to Malicious Cyber Activities* (*"Cyber Diplomacy Toolbox"), 3.*

[76] Council of the EU, *Draft implementing guidelines for the Framework on a Joint EU Diplomatic Responses to Malicious Cyber Activities*, 6-8.

[77] Council of the EU, *Declaration by the High Representative of the EU on respect for the rules-based order in cyberspace* ; Council of the EU, *Declaration by the High Representative on behalf of the European Union - call to promote and conduct responsible behaviour in cyberspace* ; Council of the EU, *Declaration by the High Representative Josep Borrell, on behalf of the European Union, on malicious cyber activities exploiting the coronavirus pandemic* (Brussels: EU, April 30, 2020).

[78] Council of the EU, *Joint statement by Presidents Tusk and Juncker and High Representative Mogherini on Russian cyber attacks* (Brussels: EU, October 4, 2018), 10.

cyber issues.[79] Moreover, 'Advancing a Global and Open Cyberspace' is one of the three prioritised areas of actions listed in the new cybersecurity, and the document advocates for the creation of an 'informal Cyber Diplomacy Network' to "promote the EU vision of cyberspace, exchange information and regularly coordinate on developments in cyberspace."[80]

From the analysis of the EU documents, it can be concluded that cyber diplomacy is very much the primary framework for the EU's external strategy concerning cybersecurity. On the one hand, cyber diplomacy is used to advance EU interests and promote its values in cyberspace issues. On the other hand, cyber diplomacy is also used to prevent and respond to cyber-attacks threatening the EU's security. The importance of cyber diplomacy is constantly repeated and increased since the EU first published a strategy for cybersecurity in 2013.

"Soft and hard power go hand in hand"

If the prominence of cyber diplomacy is well assumed in the EU's cybersecurity strategy since 2013, another trend has been observed in more recent years. It consists of coupling cyber diplomacy with 'hard power' policies. The first illustration of this trend can be found in the *Cyber Diplomacy Toolbox* and its *Implementing guidelines*. As mentioned earlier, these documents list a series of measures to prevent and respond to malicious activities in cyberspace. Amongst these measures, there is the 'possible EU support to Member States' lawful responses' that states that the EU could, if requested, provide support to a Member State victim of a cyber attack. The document explains that this possible support could consist in the use of force for self-defense in respect with Article 51 of the UN Charter.

Moreover, the document states 'restrictive measures', such as freezes of funds and arms embargoes, that the EU can impose against third countries, entities, or individuals in order to respond to a cyber attack or to "bring about a change in policy or activity by the target country, government entity or individual concerned in line with the objectives set out" by the EU. [81]

Since 2017, the EU has continued along this path and has even installed a 'cyber sanctions regime' in May 2019. This cyber sanction regime allows the EU to "impose targeted restrictive measures to deter and respond to cyber attacks with a significant effect which constitute an external threat to the EU or its member states."[82] These measures can be imposed

[79] European Commission and High Representative of the EU for Foreign Affairs and Security Policy, *The EU's Cybersecurity Strategy for the Digital Decade*, 16 ; 19.

[80] Ibid., 22.

[81] Council of the EU, *Draft implementing guidelines for the Framework on a Joint EU Diplomatic Responses to Malicious Cyber Activities*, 9.

[82] Council of the EU, *Council decision concerning restrictive measures against cyber-attacks threatening the Union or its Member States*, 4.

on states, international organizations, or any entity or individuals involved in cyber attacks in any way. The restrictive measures consist of travel bans in the EU and the freezing of the target's funds. Moreover, EU entities, individuals, and Member States are forbidden from making funds available to the targets.[83] The cyber sanction regime was extended for another year in May 2020.[84]

It should be noted that the EU has implemented the cyber sanction regimes on two occasions. In July 2020, the EU imposed these sanctions on six individuals - two of them were Chinese and four were Russian - and three entities, including the Main Centre for Special Technologies which is directly related to the Russian Army. Moreover, in October 2020, two Russian individuals and one body were added to the cyber sanction regime's list.[85] About the sanctions taken in July 2020, High Representative Josep Borrell has stated that although the EU "prioritises international cooperation and dialogue", it is not the case for every actor involved in cyberspace. Therefore, sanctions are sometimes inevitable as they "ensure that those individuals and entities are held accountable for their actions." Moreover, Borrell says that these sanctions "send a strong message to the world that [the EU] will not tolerate such cyber-attacks." He concludes by saying that the EU has the tools to protect itself and the determination to use them.[86]

Furthermore, in the new *Cybersecurity Strategy* document of 2020, there are multiple calls for using hard power as well as soft power to handle cybersecurity issues. The document states that the EU should further define its 'cyber deterrence posture' and that it should use its "political, economic, diplomatic, legal and strategic tools against malicious cyber activities".[87] The document also proposes to envisage other options for restrictive measures.

All of this indicates the EU's willingness to use its hard power in relation to its cybersecurity. This characteristic can be dated from the *Cyber Diplomacy Toolbox* and is gaining in significance since 2017. Indeed, the more recent documents suggest that this trend is going to be reinforced in the future.

Strategic autonomy

[83] Ibid., 10-15.

[84] Council of the EU, *Council extends cyber sanctions regime until 18 May 2021* (Brussels: EU, May 14, 2020).

[85] Council of the EU, *Declaration by the High Representative Josep Borrell on behalf of the EU: European Union response to promote international security and stability in cyberspace* ; Council of the EU, *Malicious cyber-attacks: EU sanctions two individuals and one body over 2015 Bundestag hack* (Brussels: EU, October 22, 2020).

[86] Borrell, Josep, "Cyber sanction: time to act," HR/VP Blog Post, July 30, 2020.

[87] European Commission and High Representative of the EU for Foreign Affairs and Security Policy, *The EU's Cybersecurity Strategy for the Digital Decade*, 17.

Concerning the idea of strategic autonomy, the analysis suggests that although this ambition is mentioned in the EU documents, the topic has not bee further explored. Only one aspect of the willingness to achieve strategic autonomy is developed in the EU cybersecurity document: cyber defence.

In the EUCSS of 2013, one of the strategic priorities is titled ‘developing cyberdefence policy and capabilities’. The idea presented in this document is a call to increase the resilience of the communication and information systems of the EU Member States. It is quoted that “cyberdefence capability development should concentrate on detection, response and recovery from sophisticated cyber threats.”[88] Following this, the Council published the first *EU Cyber Defence Policy Framework* in November 2014. However, this document is very short and concerns only the will to maintain information and communication systems of the EU and its Member States operational.[89] The *Framework* was updated in 2018. However, the core message of the *Framework* stays the same: a call to protect the communication and information systems supporting the EU institutions and its Member States.

Despite these two key documents, cyber defence capabilities of the EU is still the field of cybersecurity the least developed. In 2019, the Council of the EU has reaffirmed their willingness to strengthen the EU’s and its Member States’ cyber defence capabilities and call for further work to be done in this domain “in order to respond to evolving security challenges.”[90]

The new *Cybersecurity Strategy* of 2020 answers this call and makes several concrete proposals to boost EU cyber defence capabilities. Indeed, the doucment announces a ‘Military Vision and Strategy on Cyberspace as a Domain of Operations’ that “should further define how cyberspace as a domain of operations enables EU CSDP military missions and operations.” Cooperation between Member States is encouraged and the focus is put on Artificial Intelligence, encryption, and quantum computing. This in turn is to fulfill the overall objective of preventing, responding, and deterring cyber threats.[91]

As it can be observed, the idea of strategic autonomy in cyberspace is not very well developed. This should also be linked to the fact that in the EUGS of 2016, the idea of strategic autonomy is not well defined nor explained. Despite several key documents adopted since 2014, there is still a need, reiterated in the 2020 *Cybersecurity Strategy*, to further define the scope of

[88] European Commission and High Representative of the EU for Foreign Affairs and Security Policy, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, 11-14.

[89] Council of the EU, *Cyber Defence Policy Framework*.

[90] Council of the EU, *Council Conclusions on Security and Defence in the context of the EU Global Strategy* (Luxembourg: EU, June 17, 2019).

[91] European Commission and High Representative of the EU for Foreign Affairs and Security Policy, *The EU’s Cybersecurity Strategy for the Digital Decade*, 16-18.

the EU's actions in relation to cyber defence. Moreover, the document makes it clear that building cyber defence capabilities will be one of the key areas of action for the EU in the coming years.

Principled Pragmatism

To reiterate, the idea of 'principled pragmatism' means that the EU's actions - whether it is in cyberspace or not - should not be solely guided by the EU values but also on a realistic and pragmatic assessment of the situation and of what can be done.

In 2013, values of the EU were put at the center of EU cybersecurity: following them and promoting them are respectively the framework and one of the primary objectives of the EU's external strategy in this field. Indeed, the EUCSS states that "the EU international engagement in cyber issues will be guided by the EU's core values of human dignity, freedom, democracy, equality, the rule of law and the respect for fundamental rights", and a strategic priority of the document is to promote core EU values.[92]

With the advent of the *Cyber Diplomacy Toolbox* in 2017, the objective is no longer concerned with only promoting EU values internationally. Indeed, the document entails that the EU can condemn malicious activities in cyberspace and impose sanctions on those responsible. Moreover, it is stated that one of the guidelines for the *Cyber Diplomacy Toolbox* is to "take into account the broader context of the EU external relations with the State concerned".[93] This is reinforced by the fact that the measures can be tailored on a case-by-case basis.[94] This is significant because values no longer are the sole basis for the EU's actions. Instead, the broader context is also to be taken into account. However, this does not mean that it was not the case before 2017. What this means is that EU official documents acknowledge the need for 'principled pragmatism' in cybersecurity. This is confirmed by the creation of the cyber sanction regime in 2019.[95]

Furthermore, this does not entail that values no longer matter. Indeed, documents published afterwards still stress the importance of values as objective and guiding principles of the EU's external strategy in cyber issues. For instance, a declaration from the Council in 2018

[92] European Commission and High Representative of the EU for Foreign Affairs and Security Policy, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, 15.

[93] Council of the EU, *Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")*, 3-4.

[94] Council of the EU, *Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities*

[95] Council of the EU, *Council decision concerning restrictive measures against cyber-attacks threatening the Union or its Member States.*

highlights the importance of norms compliance in cyberspace for global stability and security.[96] More recently, the *Cybersecurity Strategy* of 2020 states that "the EU should continue [...] to promote a political model and vision of cyberspace grounded in the rule of law, human rights, fundamental freedoms and democratic values".[97]

As it can be observed, the idea of principled pragmatism as a guiding principle for the EU's external cybersecurity strategy appears with the *Cyber Diplomacy Toolbox* in 2017. Before this date, the EU's strategy was almost exclusively based on its values.

Resilience

In analysing the documents, one is bound to observe that resilience-building in third countries holds a significant role in the cybersecurity strategy of the EU externally. In the EU's cybersecurity strategy, resilience-building is linked with capacity-building in third countries. However, resilience is not intended to replace the norms-promotion agenda. As we have mentioned earlier, promoting EU values and norms is the principal objective of the EU's cybersecurity at the external level. Instead, resilience is to be implemented in addition to the promotion of EU values. This has been advocated since 2013 and the first *Cybersecurity Strategy* which states that one of the key areas of action is to develop "capacity building on cybersecurity and resilient information infrastructures in third countries."[98]

In the future documents, resilience-building in third countries gains in significance. For instance, the *Implementing guidelines* of the *Cyber Diplomacy Toolbox* consider it as a preventive measure that the EU should implement for more security at the global level.[99] The justification for resilience-building is that it "will increase the level of cybersecurity globally, with positive consequences for the EU."[100]

In the new C*ybersecurity Strategy* it is important to note that resilience-building is no longer reserved for states. Indeed, the document stresses the importance of engaging with other partners, whether its states, international organizations, civil society, or private companies. The

[96] Council of the EU, *Council conclusions on malicious cyber activities* (Brussels: EU, April 16, 2018), 3.

[97] European Commission and High Representative of the EU for Foreign Affairs and Security Policy, *The EU's Cybersecurity for the Digital Decade*, 19.

[98] European Commission and High Representative of the EU for Foreign Affairs and Security Policy, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, 16.

[99] Council of the EU, *Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities*, 6.

[100] European Commission and High Representative of the EU for Foreign Affairs and Security Policy, *Resilience, Deterrence and Defence: Building strong cybersecurity for the EU* (Brussels: EU, September 9, 2017), 19.

document recommends the creation of an EU External Cyber Capacity Building Agenda to develop coherence in EU's actions.[101]

As it can be observed, the idea of resilience is also very present in the EU's external cybersecurity strategy. Resilience-building is always linked to capacity-building and is intended to prevent instability caused by cyber attacks.

The promotion of a multilateral rules-based order under a UN framework

The promotion of a multilateral rules-based order and the importance of doing that under a UN framework has always been a key characteristic of the EU's cybersecurity external strategy. Firstly, the EU has always affirmed its willingness to promote a multi-stakeholder system of governance for cyberspace issues. This is one of the principles for cybersecurity presented in the first EU *Cybersecurity Strategy*.[102] For the EU, it is important to engage and cooperate with every actor involved in cyberspace, from sovereign states to regional organizations to civil society organizations, the academic world, or even private companies.

Secondly, the EU has adopted the position that international laws apply as much 'online' as 'offline'.[103] To support this position, the EU mentions the work done by the UN Group of Governmental Experts in the field of Information and Communication Technologies in the Context of International Security, most notably the 2010, 2013 and 2015 reports.[104] The importance of the United Nations is thus recognized for engaging in cyber issues. Moreover, the EU supports the idea that non-binding norms and rules should apply to cyber issues. In that regard, the 2020 *Cybersecurity Strategy* holds that "the EU continues to work with international partners [...] where international law, in particular the United Nations Charter, is respected, and the voluntary non-binding norms, rules and principles of responsible state behaviour are adhered to."[105]

The new *Strategy* goes further in that field as the EU aims to take forward the proposal for a political commitment on a Programme of Action to Advance Responsible State Behaviour in Cyberspace in the UN. This initiative is intended to offer "a platform for cooperation and

[101] European Commission and High Representative of the EU for Foreign Affairs and Security Policy, *The EU's Cybersecurity Strategy for the Digital Decade*, 22-23.

[102] European Commission and High Representative of the EU for Foreign Affairs and Security Policy, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, 3-4.

[103] Ibid., 15.

[104] Council of the EU, *Declaration by the High Representative on behalf of the European Union - call to promote and conduct responsible behaviour in cyberspace*.

[105] European Commission and High Representative of the EU for Foreign Affairs and Security Policy, *The EU's Cybersecurity Strategy for the Digital Decade*, 20.

exchange of best practices within the UN, and [...] to establish a mechanism to put in practice the norms of responsible state behaviour and promote capacity building."[106]

In summary, the EU has always promoted a rules-based order framework for engaging in cyber issues. The importance of the United Nations has also always been recognized. Once again, the new *Cybersecurity Strategy* proposes to go further in this field.

Inter-regionalism as a privileged way to cope with global issues

After analysing the documents, no evidence was found that inter-regionalism is privileged by the EU for coping with cybersecurity issues. Indeed, if the importance of engaging with other actors, including regional organizations, following a multi-stakeholder model of governance is reaffirmed in almost every key document on cybersecurity, inter-regionalism is never recognized as better or more favourable than other ways of cooperating with third partners. Nonetheless, the EU still acknowledges that regional organizations are key actors in cyberspace. For instance, in the EUCSS of 2013, it is written that "the EU will seek closer cooperation with organisations that are active in [cyberspace] such as the Council of Europe, OECD, UN, OSCE, NATO, AU, ASEAN and OAS."[107] This claim is reaffirmed in the 2020 *Cybersecurity Strategy*.[108]

However, it should be noted that NATO and the OSCE holds a significant place in the EU's cybersecurity strategy. About the OSCE, the EU documents state that the EU should increase its engagement within the framework of the OSCE because of the confidence-building measures adopted by this organization.[109] Concerning NATO, its role is acknowledged as the primary framework for many of Member States' defence, including in cybersecurity. As such, the EU calls for more cooperation with NATO on multiple occasions. This is especially true for the EU cyber defence capacity building and interoperability.[110] Several calls for more cooperation between NATO and the EU can be observed in that regard, such as the joint declaration of December 2016.[111] The 2020 *Cybersecurity Strategy* also acknowledges the

[106] Ibid., 20-21

[107] Ibid., 15.

[108] Ibid., 21-22.

[109] Council of the EU, *Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities*, 3.

[110] Council of the EU, *EU Cyber Defence Policy Framework*, 12 ; European Commission and High Representative of the EU for Foreign Affairs and Security Policy, *Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*, 19-20 ; Council of the EU, *EU Cyber Defence Policy Framework (2018 update),* 22.

[111] Council of the EU, *"Taking EU-NATO cooperation to a new level"* (Brussels: EU, December 13, 2016).

primary importance of NATO compared to other regional organizations and calls for further development in education, training, and exercises.[112]

As it can be observed, inter-regionalism is not put forward by the EU documents as a favored way to cope with cyber issues. However, on some topics, such as cyber defence and and confidence-building measures, the primacy of NATO and OSCE are recognized.

Focus on East and South Neighborhood

In the EUCSS of 2013, there is no focus on a specific geographical area. Indeed, if the document explains that the EU should engage with third countries and key partners, the preferred criteria for prioritization amongst the multitude of actors involved in cyberspace is values. Indeed, the document states that "the EU will place a renewed emphasis on dialogue with third countries, with a special focus on like-minded partners that share EU values."[113] Moreover, the document also recommends seeking closer cooperation with organisations that are active in this field and praises the partnership with the United States.

The same conclusions can be inferred while analyzing the *Council Conclusions on Cyber Diplomacy* as well as the *Cyber Diplomacy Toolbox*.[114] However, in 2017 the document *Resilience, Deterrence and Defence* announces a change in the EU's strategy. For the first time, it is mentioned that "the priorities for capacity-building will be the EU's neighborhood and developing countries experiencing fast growing connectivity and rapid development of threats." This new policy is reaffirmed in the 2020 *Cybersecurity Strategy*.[115] This is justified by the fact that the EU wants to link its cyber capacity building with its development agenda. Furthermore, this is coherent with the willingness of the EU to prioritize EU efforts and to be therefore more efficient and less scattered. Moreover, this could also be linked with the idea of principled pragmatism. Indeed, the EU stops favoring 'like-minded countries' and chooses instead to focus on countries where instability is most likely to affect the EU and its Member States.

However, this geographical focus concerns only cyber-capacity building. For instance, the cyber sanction regime document mentions that the EU should be concerned with any external threats to the EU. Moreover, in the area of cyber defence, the importance of NATO is

[112] European Commission and High Representative of the EU for Foreign Affairs and Security Policy, *The EU's Cybersecurity Strategy for the Digital Decade*, 22.

[113] European Commission and High Representative of the EU for Foreign Affairs and Security Policy, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, 15.

[114] Council of the EU, *Council Conclusions on Cyber Diplomacy*, 11 ; Council of the EU, *Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")*.

[115] European Commission and High Representative of the EU for Foreign Affairs and Security Policy, *The EU's Cybersecurity Strategy for the Digital Decade*, 23.

recognized. The justification for this is simply the fact that many of the EU Member States have strong ties with the transatlantic organisation.[116] Finally, when talking about "Advancing a global and open cyberspace", in other words, the norms-promotion agenda of the EU in cyberspace, there is also no geographical focus mentioned in the EU document.[117]

In summary, there is only a focus on the EU's neighborhood when it comes to cyber-capacity building.

Europeans' security and prosperity first

The relation between internal considerations and foreign policy has always been acknowledged in the EU cybersecurity documents. This should be linked to the fact that, as recognized in EU documents, Europe's society is very reliant on technology.[118] However, there is a shift in the words chosen to express this concern. Before 2017, the focus was on EU and Member States' national security interests.[119] In the *Cyber Diplomacy Toolbox*, the focus has shifted on the citizens. Indeed, the document lists the considerations to take into action for the EU diplomatic responses to malicious cyber activities. The first of these considerations is "to protect the integrity and security of the EU, its Member States and their citizens."[120] This is reaffirmed in the 2020 *Cybersecurity Strategy* as the document posits that "this strategy aims to ensure a global and open Internet with strong guardrails to address the risks to the security and fundamental rights and freedom of people in Europe."[121]

The fact that the EU stepped up its response to cyber malicious activities, firstly with the *Cyber Diplomacy Toolbox*, and secondly with the advent of the cyber sanctions regime, is a good indicator that "Europeans' prosperity, society and values" holds an increasing importance.[122] Furthermore, other calls for a stronger EU posture at the international level on

[116] Council of the EU, *EU Cyber Defence Policy Framework* ; Council of the EU, *EU Cyber Defence Policy Framework (2018 update).*

[117] European Commission and High Representative of the EU for Foreign Affairs and Security Policy, *The EU's Cybersecurity Strategy for the Digital Decade.*

[118] European Commission and High Representative of the EU for Foreign Affairs and Security Policy, *Cybersecurity of the European Union: An Open, Safe and Secure Cyberspace*, 2 ; European Commission and High Representative of the EUfor Foreign Affairs and Security Policy, *The EU's Cybersecurity for the Digital Decade*, 1.

[119] European Commission and High Representative of the EU for Foreign Affairs and Security Policy, *Cybersecurity of the European Union: An Open, Safe and Secure Cyberspace*, 11.

[120] Council of the EU, *Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")*, 4.

[121] European Commission and High Representative of the EU for Foreign Affairs and Security Policy, *The EU's Cybersecurity for the Digital Decade*, 4.

[122] Council of the EU, *Council decision concerning restrictive measures against cyber-attacks threatening the Union or its Member States*.

cybersecurity issues confirm this assumption. Of course, this has also to be linked with the increasing threats cyberspace poses for the EU, due to its increasing reliance on technology and the growing number and destructive nature of cyber attacks. In this regard, Josep Borrell has recently reiterated his concerns about the increasing vulnerability of Europeans to cyber attacks.[123]

The internal dimension has always been considered in the EU's external cybersecurity strategy. However, in 2017, the discourse shifts to encompass citizens' security.

Unity amongst EU Member States and EU institutions

The analysis of the key documents on the EU external cybersecurity strategy suggests that cooperation between Member States as well as between EU institutions is of high importance. On multiple occasions, the EU calls for better cooperation. However, it should be noted that cooperation is not a 'guiding principle' of the EU's external cybersecurity strategy like the EU values or the promotion of a multi-stakeholder model. Instead, cooperation is more considered as a way to increase and enhance the EU's efficiency in cybersecurity. This is especially true when it comes to cyber-capacity building in third countries and cyber defence capabilities in the EU. For instance, the *EU Cyber Defence Policy Framework* of 2018 notes that "there is a need to develop a common aggregated understanding on the scope of cyber defence" and describes the need for "strategic convergence."[124] Moreover, the document advocates for joint exercises and training which will improve the EU cyber defence capabilities.[125]

Once again a change of tone can be witnessed in the 2020 *Cybersecurity Strategy*. In this document, the need to focus on cooperation amongst EU Member States and EU institutions is more endorsed. Regarding the Cyber Diplomacy Toolbox, the 2020 document announces the establishment of a cyber intelligence working group to "advance strategic intelligence cooperation on cyber threats and activities". Furthermore, a 'Military Vision and Strategy on Cyberspace as a Domain of Operations' is also announced for more cooperation in the cyber defence domain. Concerning cyber capacity building in third countries, the document calls for the development of an EU External Cyber Capacity Building Agenda which is intended to, amongst other things, enhance cooperation in that field.[126]

[123] Borrell, "Make cyberspace a safer place.*"*

[124] Council of the EU, *EU Cyber Defence Policy Framework (2018 update),* 10.

[125] Ibid., 19-21.

[126] European Commission and High Representative of the EU for Foreign Affairs and Security Policy, *The EU's Cybersecurity Strategy for the Digital Decade*, 17-18 ; 22.

As it can be observed, cooperation has always been important for the EU's external cybersecurity strategy, most notably for cyber capacity building in third countries and cyber defence. However, the new *Cybersecurity Strategy* of 2020 goes further in that field and makes concrete propositions.

Findings and conclusions

The final section of this thesis will summarize the findings and provide an answer to the research question. To reiterate, the research question is: "*How coherent is the European Union's external cybersecurity strategy with the EU's willingness to become more active at the international level ?*"

First of all, the thesis has shown that the European Union has the ambition to be more active on cyber issues at an international level.

On one hand, the thesis demonstrated that some characteristics of the EU's external cybersecurity strategy correspond well to the principles and objectives set out by the European Union in order to become more active at the international level. For instance, the importance of diplomacy is recognized in the EU's external cybersecurity strategy. Indeed, cyber diplomacy is the area of action the most developed, compared to others like cyber defence. As such, it can be considered as the principal framework to describe the EU's external cybersecurity strategy.

Moreover, since 2017 and the publication of the *Cyber Diplomacy Toolbox*, the EU has also demonstrated its willingness to use other types of tools available to meet its objective. This approach is coherent with the EU's ambition to use soft as well as hard power.

This is also the case for the idea of principled pragmatism. Indeed, the analysis has demonstrated that promoting EU values abroad remains one of the principal objectives of the EU's external cybersecurity strategy to prevent instability in cyberspace. However, in 2017, the EU has given itself other means to prevent and respond to malicious cyber activities, such as confidence-building measures or sanctions. Moreover, whereas before 2017, the EU's strategy stated that values were to be the guiding principles of the EU's actions in cyberspace, since 2017, the EU strategy cites that the broader context also needed to be taken into account. In other words, the idea of principled pragmatism starts to appear in 2017 in the EU's external cybersecurity strategy but values.

The EU has also always promoted a multilateral rules-based order under a UN framework to handle cyber issues. Indeed, the EU holds and promotes the idea that international laws, as well as non-binding norms, apply also in cyberspace. Moreover, the primacy of the United Nations has always been recognized.

The link between EU external actions and its internal security has always been acknowledged. In other words, the rationale for the EU's external cybersecurity strategy is and has always been the EU's security. However, since 2017, the focus has shifted from 'protecting the national interests of Member States' to 'protecting the citizens'.

Concerning the need for Member States and EU institutions to be united, it was shown that this was always praised in the EU external cybersecurity strategy. Cooperation and coordination are considered as ways to increase the EU's actions' efficiency. In the 2020 *Cybersecurity Strategy*, this need for cooperation is more highlighted than ever.

On the other hand, for the idea of resilience, the picture is more mixed. Indeed, while the principle of resilience holds a significant place in the EU's external cybersecurity strategy to prevent instability in cyberspace, it is not intended to replace the norms-promotion agenda. Instead, the two approaches are adopted.

On another hand, some characteristics do not correspond, or only partly, with the principles set out in the theoretical framework. For instance, in the EU's external cybersecurity strategy, inter-regionalism is not considered as a privileged way to handle cyber issues. Of course, the EU promotes dialogue with every key partner following a multi-stakeholder model but inter-regionalism is not viewed as more favorable than any other framework. This has to be linked with the fact that coping with cyber issues requires engagement with every actor involved, which is not possible if we prioritize the inter-regionalism framework. Still, some regional organizations hold a special place in the EU's external cybersecurity strategy. This is the case for NATO and the OSCE.

This is also true regarding the focus on the EU's neighbourhood. Indeed, it is difficult to address cyber issues only in one geographical zone. The engagement has to be global. However, in 2017, the EU's external cybersecurity strategy mentions that for cyber-capacity building in third countries, the EU will focus on its close neighborhood. This can be justified by the fact that the EU needs to prioritize in order to use its limited resources as most efficiently as possible.

Moreover, the idea of strategic autonomy is not developed in the EU's cybersecurity external strategy. Only one aspect is discussed: cyber defence. Yet, this aspect is also very underdeveloped.

Moreover, the thesis demonstrates that 2017 and the publication of the *Cyber Diplomacy Toolbox* is a turning point in the EU's external cybersecurity strategy. For sure this has to be linked with the publication of the *European Union Global Strategy* of 2016. In 2017, we witness a reorientation of the EU's external cybersecurity strategy to be more coherent with the principles and ideas proposed by the EUGS. This is true for some aspects like principled pragmatism and the coupling of soft power with hard power. If some aspects were already present in the EU's external cybersecurity strategy prior 2016, they have been reinforced since.

It concerns, for instance, the importance of diplomacy or the promotion of a multilateral order under a UN framework.

However, some principles still appear to be missing or are present in only a limited manner, such as resilience, inter-regionalism, and focusing on the neighborhood. Yet, it should be noted there are valid reasons that justify the lack of development around these principles. For instance, the limited resources available and the fact that cyber issues have to be dealt with globally. The idea of strategic autonomy, notably concerning EU cyber defence, is still greatly underdeveloped. However, it seems that the 2020 *Cybersecurity Strategy* intends to fill this gap in the EU's external cybersecurity strategy. Indeed, the new EU document goes a step further as it makes concrete proposals to increase every aspect and principles and to enhance the coherence between the EU's external cybersecurity strategy and its willingness to be more active at the international level as well as its guiding principles to achieve this objective.

In answering the research question, this thesis has explored one aspect of the relationship between the EU's ambition to become more active at the international level and the EU's external cybersecurity strategy. In turn, it offers a first step in addressing the gap in the literature around this topic and encourages further research in the field. For instance, an upcoming contribution could explore the coherence between EU's actions (instead of its strategy) in cybersecurity and the EU's willingness to be more active on a global stage.

Moreover, it offers EU policymakers a basis upon which to assess the EU's external cybersecurity strategy and improve it. One specific aspect is the idea of strategic autonomy, and notably the cyber defence capabilities of the EU, which need to be developed in the forthcoming years.

Bibliography

Primary sources

Borrell, Josep. "A stronger European Union within a better, greener and safer world - key principles that will be guiding my mandate.*"* HR/VP Blog Post. December 1, 2019. https://eeas.europa.eu/headquarters/headquarters-homepage/71265/stronger-european-union-within-better-greener-and-safer-world-key-principles-will-be-guiding_en.

---. "Cyber sanctions: time to act." HR/VP Blog Post. July 30, 2020. https://eeas.europa.eu/headquarters/headquarters-homepage/83627/cyber-sanctions-time-act_en

---. "Make cyberspace a safer place." HR/VP Blog Post. December 17, 2020. https://eeas.europa.eu/headquarters/headquarters-homepage/90747/make-cyberspace-safer-place_en

Council of the European Union. *European Security Strategy*. *A Secure Europe in a Better World*. Brussels: European Union, December 8, 2013.

---. *EU Cyber Defence Policy Framework*. Brussels: European Union, November 18, 2014.

---. *Council Conclusions on Internet Governance*. Brussels: European Union, November 27, 2014.

---. *Council Conclusions on Cyber Diplomacy*. Brussels: European Union, February 11, 2015.

---. *"Taking EU-NATO cooperation to a new level".* Brussels: European Union, December 13, 2016.

---. *Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox").* Brussels: European Union, June 19, 2017.

---. *Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities*. Brussels: European Union, October 9, 2017.

---. *Council conclusions on malicious cyber activities.* Brussels: April 16, 2018.

---. *Joint statement by Presidents Tusk and Juncker and High Representative Mogherini on Russian cyber attacks.* Brussels: European Union, October 4, 2018.

---. *EU Cyber Defence Policy Framework (2018 update)*. Brussels: European Union, November 19, 2018.

------. *Declaration by the High Representative on behalf of the EU on respect for the rules-based order in cyberspace.* Brussels: European Union, April 12, 2019.

---. *Council decision concerning restrictive measures against cyber-attacks threatening the Union or its Member States*. Brussels: European Union, May 14, 2019.

---. *Council Conclusions on Security and Defence in the context of the EU Global Strategy.* Luxembourg: European Union, June 17, 2019.

---. *Declaration by the High Representative on behalf of the European Union - call to promote and conduct responsible behaviour in cyberspace.* Brussels: European Union, February 21, 2020.

---. *Declaration by the High Representative Josep Borrell, on behalf of the European Union, on malicious cyber activities exploiting the coronavirus pandemic.* Brussels: European Union, April 30, 2020.

---. *Council extends cyber sanctions regime until 18 May 2021.* Brussels: European Union, May 14, 2020.

---. *Declaration by the High Representative Josep Borrell on behalf of the EU: European Union response to promote international security and stability in cyberspace.* Brussels: European Union, July 30, 2020.

---. *Malicious cyber-attacks: EU sanctions two individuals and one body over 2015 Bundestag hack.* Brussels: European Union, October 22, 2020.

European Commission. *The von der Leyen Commission: for a Union that strives for more*. Brussels: European Union, September 10, 2019.

---. *Speech by President-elect von der Leyen in the European Parliament Plenary on the occasion of the presentation of her College of Commissioners and their programme*. Strasbourg: European Union, November 27, 2019.

---. *Mission letter to Josep Borrell, High Representative of the Union for Foreign Affairs and Security Policy/Vice-President of the European Commission.* Brussels: European Union, December 1, 2019.

---. *New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient.* Brussels: European Union, December 16, 2020.

European Commission and High Representative of the European Union for Foreign Affairs and Security Policy. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. Brussels: European Union, 2013.

---. *Resilience, Deterrence and Defence: Building strong cybersecurity for the EU.* Brussels: European Union, September 9, 2017.

---. *The EU's Cybersecurity Strategy for the Digital Decade*. Brussels: European Union, December 16, 2020.

European External Action Service. *Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the EU's Foreign and Security Policy*. Brussels: European Union, June 2016.

von der Leyen, Ursula. *A Union that strives for more. My agenda for Europe : Political guidelines for the next European Commission 2019-2024.* Brussels: European Union, October 9, 2019.

Secondary Sources

Barrinha, André, and Thomas Renard. "Cyber-diplomacy: the making of an international society in the digital age." *Global Affairs* 3, no. 4-5 (2017): 353-364.

Bendiek, Annegret. "European Cyber Security Policy." Stiftung Wissenschaft und Politik. Research Paper 13, October 2012.

---. "The EU as a Force for Peace in International Cyber Diplomacy." Stiftung Wissenschaft und politik. SWP Comment 19, April 2018.

Biscop, Sven. "Strategy. What can Europe do, what does Europe want?." Chap. 2 in *European Strategy in the 21st Century. New Future for Old Power*, 21-36. London, UK: Routledge, 2018.

Bowen, Glenn. “Document Analysis as a Qualitative Research Method.” *Qualitative Research Journal* 9, no. 2 (2009): 27-40.

Calleri, Martina. “The European Union as a Global Actor in Cyberspace: Can the Cyber Sanctions Regime Effectively Deter Cyber-Threats?.” *Romanian Cyber Security Journal* 2, no. 2 (Fall 2020): 3-9.

Carrapico, Helena, and André Barrinha. “The EU as a Coherent (Cyber)Security Actor?.” *Journal of Common Market Studies* 53, no. 6 (2017): 1254-1272.

---. “European Union cyber security as an emerging research and policy field.” *European Politics and Society* 19, no. 3 (2018): 299-303.

Davis Cross, Mai’a K. “The EU Global Strategy and diplomacy.” *Contemporary Security Policy* 37, no. 3 (2016): 402-413.

Dijkstra, Hylke. “Introduction: one-and-a-half cheers for the EU Global Strategy.” *Contemporary Security Policy* 37, no. 3 (2016): 369-373.

Dunn Cavelty, Myriam. “Europe’s cyber-power.” *European Politics and Society* 19, no. 3 (2018): 304-320.

Giusti, Serena. “The European Union Global Strategy and the EU’s Maieutic Role.” *Journal of Common Market Studies* 58, no. 6 (2020): 1452-1468.

Howorth, Jolyon. “EU Global Strategy in a changing world: Brussels’ approach to the emerging powers.” *Contemporary Security Policy* 37, no. 3 (2016): 389-401.

Ivan, Paul. “Responding to cyberattacks: Prospects for the EU Cyber Diplomacy Toolbox.” European Policy Centre. Discussion Paper, March 18, 2019.

Julien, Heidi. “Content Analysis.” In *The SAGE Encyclopedia of Qualitative Research Methods*, edited by Lisa M. Given, 121-122. Thousand Oaks, CA: SAGE Publications, 2012.

Jorgensen, Knud-Erik, and Yonatan Schvartzman. “The EU as a Global Actor.” Chap. 1 in *The European Union as a Global Health Actor,* edited by Thea Emmerling, Ilona Kickbush and Michaela Told, 1-20. Singapore: World Scientific, 2016.

Kovács, László. “Cyber Security Policy and Strategy in the European Union and NATO.” *Land Forces Academy Review* 23, no. 1/89 (2018): 16-24.

Lamont, Christopher. “Qualitative Methods in International Relations.” Chap. 5 in *Research Methods in International Relations*, 77-95. Thousand Oaks, CA: SAGE Publications, 2015.

Levy, Jack S. “Qualitative Methods in International Relations.” In *Evaluating Methodology in International Studies,* edited by Frank P. Harvey and Michael Brecher, 131-160. Ann Arbor, MI: University of Michigan Press, 2002.

Mälksoo, Maria. “From the ESS to the EU Global Strategy: external policy, internal purpose.” *Contemporary Security Policy* 37, no. 3 (2016): 374-388.

Moret, Erica, and Patryk Pawlak. “The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime?.” European Union Institute for Security Studies. Brief 24, July 2017.

Novotná, Tereza. “The EU as a Global Actor: United We Stand, Divided We Fall.” *Journal of Common Market Studies* 55 (September 2017): 177-191.

Odermatt, Jed. “The European Union as a cybersecurity actor.” Chap. 17 in *Research Handbook on the EU’s Common Foreign and Security Policy*, edited by Steven Blockmans and Panos Koutrakos, 354-373. Cheltenham, UK: Edward Elgar, 2018.

Pishchikova, Kateryna, and Elisa Piras. “The European Union Global Strategy: What Kind of Foreign Policy Identity?.” *The International Spectator* 52, no. 3 (2017): 103-120.

Renard, Thomas. “The European Union: A New Security Actor.” Robert Schuman Centre for Advanced Studies, EUI Working Paper 45. April 2014.

---. “The rise of cyber-diplomacy: the EU, its strategic partners and cyber-security.” European Strategic Partnerships Observatory. Working Paper 7. June 2014.

---. “EU cyber partnerships: assessing the EU strategic partnerships with third countries in the cyber domain.” *European Politics and Society* 19, no. 3 (2018): 321-337.

Sliwinski, Krzysztof Feliks. “Moving beyond the European Union’s Weakness as a Cyber-Security Agent.” *Contemporary Security Policy* 35, no. 3 (2014): 468-486.

Smith, Karen E. “A European Union global strategy for a changing world?.” *International Politics* 54 (2017): 503-518.

Sus, Monika. “Institutional innovation of EU’s foreign and security policy: Big leap for EU’s strategic actorness or much ADO about nothing?.” *International Politics* 56 (2019): 411-425.

Tereszkiewicz, Filip. “The European Union as a normal international actor: an analysis of the EU Global Strategy.” *International Politics* 57, no. 1 (2020): 95-114.

Tocci, Nathalie. “The making of the EU Global Strategy.” *Contemporary Security Policy* 37, no. 3 (2016): 461-472.

---. “Resilience and the role of the European Union in the world.” *Contemporary Security Policy* 41, no. 2 (2020): 176-194.