MYKOLAS ROMERIS UNIVERSITY

SCHOOL OF LAW

INSTITUTE OF INTERNATIONAL AND EUROPEAN UNION LAW

ELEONOR BONFILS

(EUROPEAN UNION LAW AND GOVERNANCE)

THE EU CYBER DIPLOMACY TOOLBOX: IMPACT ON THE EU SANCTIONS REGIME

Master thesis

Supervisor –

Prof. dr. Regina Valutytė

Vilnius, 2022

Table of contents

List of Abbreviations

AFSJ	Area of Freedom Security and Justice
CFSP	Common Foreign and Security Policy
CJEU	Court of Justice of the European Union
Cyber Diplomacy Toolbox	Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities
Cyber sanctions regime	Legal framework for restrictive measures against cyber-attacks threatening the Union or its Member States
EC3	European Cybercrime Centre
EEAS	European External Action Service
ENISA	EU Agency for Network and Information Security
EU	European Union
EUCSS	EU Cybersecurity Strategy
NATO	North Atlantic Treaty Organization
NIS Directive	Directive on Security of Network and Information Systems
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
UK	United Kingdom
UN	United Nations
UNGGE	United Nations' Group of Governmental Experts
US	United States

Introduction

According to the former president of the European Commission Jean-Claude Juncker "*Cyber-attacks can be more dangerous to the stability of democracies and economies than guns and tanks. […] Cyber-attacks know no borders and no one is immune.*"[1].[2] From these words pronounced in 2017, Jean-Claude Juncker raises the danger of cyber-attacks in our digital societies and the disastrous consequences they have on both sovereign institutions and the security of citizens.

This situation is even more worrying as cyber-attacks are on the rise. As a matter of fact, in the recent years, cyber incidents and cyberattacks have increased significantly in various and important sectors such as transport, energy, health and finance.[3] Our modern societies, businesses, health care systems, financial systems rely on almost merely digital networks and information systems. Obviously, the Covid-19 pandemic has been a key event in the acceleration and change towards a digital world – for better or for worse. Thus, this shift towards a digitalisation of our economy and society represents an incredible opportunity for cyberattacks' perpetrators – such as state or non-state actors – to obtain important information on sensitive subjects.[4] Statistics from the EU Agency for Network and Information Security (ENISA) show that both malware and ransomware attacks have been increasing again from April 2021 up to July 2022.[5] Indeed, in June 2022, adware trojans, a specific malware, were downloaded around 10 million times.[6] Overall, the Public Administration and Finance sectors are the most impacted by the cyber-attacks.[7] These attacks constitute a major threat to our democracies, economies, and personal privacies.

This increase of cyberattacks shows the shift which our societies are confronted with. Especially, the fact that cyberattacks, understood as "a deliberate use of malicious software for

[1] "European Commission President Jean-Claude Juncker. State of the Union Address," 13 September 2017, https://ec.europa.eu/commission/presscorner/api/files/document/print/en/speech_17_3165/SPEECH_17_3165_EN.pdf
[2] "Resilience, Deterrence and Defence: Building strong cybersecurity in Europe," European Commission, *State of the Union*, 2017, 1, www.consilium.europa.eu/media/21480/cybersecurityfactsheet.pdf.
[3] Ibid.
[4] "Recent cyber-attacks and the EU's cybersecurity strategy for the digital decade," European Parliament, *Plenary*, 1 June 2021, 1, https://www.europarl.europa.eu/RegData/etudes/ATAG/2021/690639/EPRS_ATA(2021)690639_EN.pdf
[5] "ENISA Threat Landscape 2022," European Union Agency for Cybersecurity, November 2022, 16, https://doi.org/10.2824/764318
[6] Ibid., 52
[7] Ibid., 16

exploiting or altering computer code, data or logic to cause harm"[8], constitute a new tool of warfare. In other words, there is a shift from a traditional military armed conflict to a "hybrid warfare".[9] A current example is the Ukrainian war of 2022 where Ukraine has suffered numerous cyberattacks orchestrated by Russia.[10] In truth, these cyberattacks begun in 2014 with the annexation of Crimea and more than 500,000 cyberattacks took place since 2020.[11] Actually, the conflict between Russia and Ukraine impacted and reshaped the cybersecurity threat landscape.[12] Indeed, during the Ukraine-Russia conflict, there was significant increase of cybercrimes and phishing as a new tool for warfare.[13]

In response to these increasing cyberattacks, the EU and its members states have acted to respond to and deter these malicious threats. Thus, since 2013, the EU launched several strategies and structures to cope with cybercrimes, build a strong cyber resilience and to respond to cyberattacks aimed at the Member States and/or the EU's institutions, agencies, and bodies.[14] The EU's responsiveness shows its concern and preoccupation regarding cyberattacks. Thus, among the EU's resilience, deterrence, and response to cyber-attacks, the European Commission and the High Representative have proposed a "framework for a Joint EU Diplomatic Response to Malicious Cyber Activities and measures to strengthen international cooperation on cybersecurity, including deepening of the cooperation between the EU and NATO".[15] This proposal was completed on 19 June 2017 when the Council of the European Union adopted the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities also known as *the Cyber Diplomacy Toolbox*. The latter is part of the EU's approach to cyber diplomacy, within the Common Foreign and Security Policy (CFSP). The triggering event for this Cyber Diplomacy Toolbox was the WannaCry and NotPetya cyberattacks that happened in 2017.

The idea behind this framework is to mitigate cyberattacks and to influence the behaviour of potential long-term aggressors. It is a diplomatic response to cyberattacks which

[8] Patryk Pawlak, Eneken Tikk, and Mika Kerttunen, "Cyber conflict encoded: the EU and conflict prevention in cyberspace," Conflict series, *European Union Institute for Security Studies*, 7 (2020): 2, https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%207_Cyber.pdf
[9] Yves Doutriaux, "La boussole stratégique et l'invasion de l'Ukraine par la Russie," *Revue de l'Union européenne* 661 (2022): 471
[10] Luke Harding, ""Ukraine Hit By "Massive" Cyber-Attack on Government Websites," *The Guardian*, January 14, 2022, https://www.theguardian.com/world/2022/jan/14/ukraine-massive-cyber-attack-government-websites-suspected-russian-hackers
[11] Ibid.
[12] "ENISA Threat Landscape 2022," op. cit., 4
[13] Ibid., 5
[14] "Resilience, Deterrence and Defence: Building strong cybersecurity in Europe," op. cit., 1
[15] Ibid.

provides for five types of measures as essential tools of the CFSP, including preventive measures, cooperative measures, stability measures, restrictive measures and supportive measures within the CFSP.

First, the preventive measures are a classical tool in EU diplomacy. In terms of cyberattacks prevention, the EU emphasises the importance of Confidence Building Measures (CBMs), including EU cyber capacity building in third states.[16] By enhancing transparency and predictability, they aim at preventing a potential cyberattack from arousing. They will allow for both a rapid response for mitigating immediate threats and for long term resilience and cyber threats' reducing. Moreover, preventive measures include awareness-raising on EU policies such as EU démarches and EU-led political and thematic dialogues, particularly cyber or security dialogues.[17]

Second, the cooperative measures consist of EU-led political and thematic dialogues or through démarches by the EU Delegations in order to first signal the graveness of the situation for the EU and second to facilitate the peaceful resolution of an ongoing incident.[18] These cooperative measures are essentially useful for Member States to help working on diplomatic relationships with third states in cybersecurity.

Third, the stability measures comprise statements and declarations expressing or condemning cyber threats and cyberattacks on behalf of the EU.[19] These can be statements by the High Representative of the EU, Council of the EU conclusions and diplomatic démarches by the EU delegations. All serve the same purpose which is to signal and underline awareness of potential consequences of cyberattacks.

Fourth, restrictive measures which refer to sanctions as part of the CFSP.[20] They shall be imposed following the two-step approach required by EU Treaties. First on the basis of a Council Decision adopted under article 29 TEU, then a Council Regulation adopted under article 215 TFEU. Thus, when it comes to cyber deterrence, the EU may impose sanctions in response to malicious cyber acts, if deemed necessary. Respecting the principle of proportionality, restrictive measures include travel bans, arms embargoes and freezing funds or

[16] "Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities," Council of the European Union, OJ 13007/17, 9 October 2017, https://data.consilium.europa.eu/doc/document/ST-13007-2017-INIT/en/pdf
[17] Ibid.
[18] Ibid.
[19] Ibid.
[20] Ibid.

economic resources. These EU restrictive measures as part of the Cyber Diplomacy Toolbox represent the most remarkable and striking instrument in the EU's cyber diplomatic strategy.

Finally, the supportive measures which consists of the possible EU support to Member States' lawful responses.[21] Indeed, if an EU Member State is victim of a cyberattack, it can lawfully resort to non-forcible and proportionate countermeasures. This may go as far as the use of article 51 of the Charter of the United Nations – which provides for the right to self-defence[22] – or article 42(7) TEU[23] – which provides for aid and assistance by other EU member states.

Among these measures, the most striking and symbolic is the new cyber sanctions regime adopted by the Council of the EU on 17 May 2019.[24] The Council established a framework for the EU to impose targeted restrictive measures to deter and counter cyber-attacks that pose an external threat to the EU or its Member States.[25] Restrictive measures may also be imposed in response to cyber-attacks against third States or international organisations where such measures are deemed necessary to achieve the objectives of the CFSP.[26] Yet, it is only in 2020 that EU imposes its first ever sanctions following cyber-attacks.

The topic of this thesis focuses on the impact of the Cyber Diplomacy Toolbox on the EU sanctions regime. Therefore, and logically, the thesis will consider and analyse only the legal framework for restrictive measures against cyber-attacks established by the Cyber Diplomacy Toolbox, not the other four above-mentioned measures. Subsequently, the new cyber sanctions regime and the two packages of EU cyber sanctions adopted in 2020 are of particular importance for further analysis. Moreover, as the Cyber Diplomacy Toolbox is an instrument adopted under the CFSP, the understanding of the intergovernmental nature and its effect on the adoption of cyber sanctions is significant for the purpose of this thesis. Finally, any EU sanctions regime is subject to judicial review by the Court of Justice of the European Union (CJEU). Hence, this thesis will also focus on the judicial standards set by the CJEU and

[21] Ibid.
[22] "Charter of the United Nations," 26 June 1945, Article 51, https://www.un.org/en/about-us/un-charter/full-text
[23] "Consolidated Version of the Treaty on European Union signed on 13 December 2007," OJ C 326/13, 26 October 2012, Article 42, paragraph 7, https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0023.02/DOC_1&format=PDF
[24] "Cyber-attacks: Council is now able to impose sanctions," Council of the European Union, *Press release*, 17 May 2019, https://europa.eu/!yp76kW
[25] Ibid.
[26] Ibid.

its influence on the autonomous cyber sanctions' regime and especially regarding the evidence collection for cyber sanctions.

Problems of research

Consequently, the Cyber Diplomacy Toolbox's impact on the EU sanctions regime raises several questions which are the following.

First, to what extent the legal framework for the new cyber sanctions regime differs from the general framework for restrictive measures?

Second, whether the intergovernmental nature of the CFSP, which the Cyber Diplomacy Toolbox is part of, impedes the effectiveness of the EU cyber sanctions regime? Whether the policy of attribution as a whole process constitutes a limit as to the credibility of EU cyber diplomacy?

Another question is if the evidence collection issue constitutes an important legal loophole with regards the rule of law standard set by the CJEU?

Finally, whether the Cyber Diplomacy Toolbox contributes distinctively to the EU sanctions regime?

Aim and objectives of research

The aim of the thesis is to determine whether the EU cyber sanctions regime within the Cyber Diplomacy Toolbox contributes distinctively to the EU sanctions regime given its legal framework and the intergovernmental nature of the CFSP.

In pursuance of the identified aim the following objectives are established:

- To determine and analyse the nature and scope of the cyber sanctions regime.
- To assess whether the criteria for listing a targeted person are clear and precise enough to enable the Council to adopt a sanction.
- To determine and assess whether the CFSP nature on which the EU cyber sanctions regime is based upon will impede the credibility of the Cyber Diplomacy Toolbox. Thus, an analysis of the attribution policy preliminary to the adoption of cyber sanctions will be necessary.

- To determine whether the decisions of the Council based on confidential information are sufficiently evidenced to succeed in the CJEU's judicial review given the judicial standards set by the CJEU with regards cyber sanctions.
- To assess whether the cyber sanctions could be based on the Area of Freedom, Security and Justice (AFSJ) instead of the CFSP.

Relevance of the final thesis

The area of law is still evolving and is therefore innovative. Indeed, only the United States (US) and the EU have developed and adopted a framework of cyber sanctions. The US were the first to adopt an American cyber sanctions framework in April 2015 against persons responsible for malicious cyber-enabled activities. The EU followed by adopting its own autonomous cyber sanctions regime in 2019. Still, these are the two only cyber sanctions regimes in place on the international scene.

The EU cyber sanctions regime is a recent and unique system of cyber sanctions in Europe that deserves in-depth analysis. Therefore, to develop, and perhaps encourage States to develop, a sustainable and effective system of cyber sanctions, it is necessary to analyse and criticise the current state of the EU cyber sanctions regime in order to adapt and find a solution for its effectiveness due to ongoing social changes. Cyberattacks raise new legal challenges, especially regarding the protection of our personal data, but more generally the protection of our democracies and the rule of law. Thus, this thesis will assess the Cyber Diplomacy Toolbox and the EU cyber sanctions regime to enable more effective use and perhaps to encourage other states to develop their own.

Scientific novelty and overview of the research on the selected topic

The Cyber Diplomacy Toolbox is quite a recent instrument in the EU resilience deterrence strategy. As a matter of fact, the EU has used the cyber sanctions regime only twice, both in 2020. Since then, no other cyber sanctions have been adopted by the EU.

The Cyber Diplomacy Toolbox and the cyber sanctions regime are recent legal instruments. Therefore, not the whole legal issues the cyber sanctions raise have been examined by the doctrine. Scholars converge regarding the reserved effectiveness of the new regime. That

is the case for Annegret Bendiek[27], Matthias Schulze[28], Patryk Pawlak[29], and Thomas Biersteker[30] who claim that the EU is confronted with challenges intrinsically linked with the CFSP nature of the cyber sanctions regime.

In general, most legal scholars focused on what innovation the Cyber Diplomacy Toolbox brought and whether the two packages of cyber sanctions adopted in 2020 were effective. Since then, however, an extension has been agreed so that the regime will continue until 2025. Thus, new challenges and legal issues arise.

This thesis therefore analyses the whole legal framework of the cyber sanctions regime. The thesis compares it with the general framework of EU restrictive measures to determine whether its contribution justifies a special framework specific for the deter of cyber-attacks. Does the cyber-sanctions regime contribute significantly to the point of becoming a special and permanent sanctions regime? Will it become a benchmark regime that will lead Member States to adopt national legislation in line with the spirit of the Cyber Diplomacy Toolbox?

It is true that the doctrine focused on one part of the problem with the EU cyber sanctions regime, namely public attribution. It is an important issue that undeniably deserves to be raised. However, through this thesis, the author takes the issue further by asking whether the intergovernmental nature of the CFSP, on which the Cyber Diplomacy Toolbox and thus the cyber sanctions regime is based on, is not the real problem of the cyber sanctions regime's effectiveness.

Furthermore, another aspect the literature, notably Yuliya Miadzvetskaya[31], has analysed in a succinct way is the judicial standards set by the CJEU in relation to the decisions of the Council of the EU adopting cyber sanctions. This thesis will distinguish itself by linking the problem of the lack of evidence collected for the cyber-attacks – due to the lack of European autonomy of cyber intelligence services – with its contribution to the EU sanctions regime.

---

[27] Annegret Bendiek, and Matthias Schulze, "Attribution: a major challenge for EU cyber sanctions. An analysis of WannaCry, NotPetya, Cloud Hopper, Bundestag Hack and the Attack on the OPCW," *SWP Research Paper* 11 (2021): 8, doi:10.18449/2021RP11

[28] Ibid.

[29] Patryk Pawlak, and Thomas Biersteker, "Guardian of the Galaxy: EU cyber sanctions and norms in cyberspace," *Chaillot Paper* 155 (2019): 52-53, https://www.iss.europa.eu/sites/default/files/EUISSFiles/cp155.pdf

[30] Ibid.

[31] Yuliya Miadzvetskaya, "Chapter 12: Challenges of the cyber sanctions regime under the common foreign and security policy (CFSP)," In Security and Law: Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security, A. Vedder, J. Schroers, C. Ducuing, P. Valcke (Cambridge: Cambridge University Press, 2019), 282

Significance of research

This thesis can be useful for both the private and public sectors. Indeed, this study highlights the importance of coordination between different institutional and state levels to link their information efforts in an efficient manner. Thus, both the EU, the Member States and the cyber companies may find that considerations presented in the present research are useful for future cyberattacks that should be subject to sanctions.

As cybersecurity is a constant evolving area, legal scholars, the institutions and companies may continue to deepen the analysis of (future) EU cyber sanctions so as to maintain an open, free, secure and stable cyberspace.

Research methodology

To achieve the aim of the thesis, the following methods were used:

- The description method was used for providing a general overview of the contextual background leading to the adoption of Cyber Diplomacy Toolbox by the EU, and further the cyber sanction regime with the Decision 2019/797 and Regulation 2019/796 adopted by the Council of the EU. To explain the EU sanction regime in general, and more specifically article 29 of the Treaty on European Union (TEU) and article 215 of the Treaty on the Functioning of the European Union (TFEU). The method was also used to define the principle of due diligence in international law, which is enshrined in the Cyber Diplomacy Toolbox.
- The systematic method was used to clarify legal documents and publications of scholars. It is also employed to assess, organise, and select different sources of information in order to identify the most relevant issues of the thesis. It was also applied for analysing and determining whether the CFSP pillar, which is in its nature intergovernmental, is a limit to the credibility of the EU cyber sanctions regime.
- The comparative method was used to compare the opinions and analysis made by scholars with regards the similar legal and diplomatic issues. The method was employed in relation with the Decision 2019/797 and Regulation 2019/796 adopted by the Council of the EU.
- The linguistic method was used in interpreting the provisions of legal framework for restrictive measures against cyber-attacks threatening the Union or its Member States (i.e. Decision 2019/797 and Regulation 2019/796), the cyber sanctions adopted by the

EU, the articles of the EU Treaties and the caselaw of the CJEU in order to understand the meaning of the legal concepts and criteria.

- The critical method was used to determine whether the cyber sanctions could fall under the scope of the AFSJ instead of the CFSP to circumvent the intergovernmental obstacles inherent to cyber sanction regime.

Structure of research

The thesis is divided into the following parts: introduction, four substantial parts that are divided into two subsections which are further divided into smaller sections and finally the conclusions.

The first part of this thesis describes and analyses the EU's strategic deployment in cyber-deterrence which led to the adoption of the Cyber Diplomacy Toolbox in 2017. This part is divided into two subparts. Following a cyber deterrence and resilience approach, the EU institutions responded and developed a strategy which aimed at adopting several instruments in order to cope with cyber malicious acts (1.1.). Among them, the most notable and significant for the purpose of this thesis is the Cyber Diplomacy Toolbox from 2017, a CFSP instrument, which enshrines the resilience approach (1.2.).

The second part focuses on the legal framework of the newly established sanctions regime, i.e., the EU cyber sanctions regime. This part is divided into two subparts. It first explains the nature of the regime stemming from both Decision (CFSP) 2019/797 – based on article 29 TEU – and Regulation (EU) 2019/796 – based on article 215 TFEU (2.1.). Then, the thesis analyses the scope of the cyber sanctions regime on the basis of the two current and only cyber sanctions packages the EU has imposed up until now (2.2.).

The third part of this thesis argues that the intergovernmental nature of the CFSP constitutes a limit to the effectiveness of the cyber sanctions regime. This part is divided into three subparts. It first explains that as a CFSP instrument, EU's cyber deterrence and security strategy follows the international law principle of due diligence which the Cyber Diplomacy Toolbox has enshrined (3.1.). Further, it analyses the policy of attribution, indispensable for the EU to adopt the cyber sanctions, which remains a legal challenge undermining the principle of due diligence (3.2.). Finally, it argues that the collection of substantial evidence appears to be a loophole for the cyber sanctions' judicial review (3.3.).

The fourth and last part raises the delimitation issue between the CFSP and the AFSJ with regards cyber sanctions. This part is divided into two subparts. For a better understanding, it is important first to address the decision-making procedures of both the CFSP and AFSJ (4.1.). Then, to raise the border clash between the CFSP and the AFSJ as a potential solution to overcome the intergovernmental obstacles (4.2.).

Defence statements

At present, given the legal framework of the cyber sanctions regime and the nature of the CFSP, the Cyber Diplomacy Toolbox does not contribute distinctively to the EU sanctions regime.

1. The EU diplomatic strategy: a strong will for cyber-deterrence

Following a cyber deterrence and resilience approach, the EU institutions responded and developed a strategy which aimed at adopting several instruments in order to cope with cyber malicious acts (1.1.). Among them, the most notable and significant for the purpose of this thesis is the Cyber Diplomacy Toolbox from 2017, a CFSP instrument, which enshrines the resilience approach (1.2.).

1.1. The EU institutional responsiveness against cyber malicious acts of states and non-states actors

The digitalisation of our society and economy has brought many benefits to citizens and businesses. Digitalisation offers important opportunities for economic growth and for facilitating social exchanges and integration. However, this change towards a digital society presents risks that are not without consequences. Indeed, cyberattacks are on the rise and are an integral part of our daily lives; both for companies, for governmental institutions and for citizens.

The increase of cyberattacks for the past ten years is evidenced by the malicious behaviours from state and non-state actors in the cyberspace so as to achieve their political goals.[32] This is achieved mostly by the growing use of ransomware, the use of malicious malware, cyberattacks against specific infrastructures or cyberespionage.[33] Malicious cyberoperations directed against EU member states or EU institutions, generally originating by China, Russia, Iran, are obviously threatening the security of the cyberspace and its users.[34] Thus, such above-mentioned malicious cyber activities have triggered the EU's reaction and response against these acts in breach of international law according to article 2.4 of the UN Charter which provides for the prohibition of the threat or unilateral use of force in international relations.

The EU has adopted a responsive strategy, based on a resilience and deter position, against cyber malicious acts of states and non-states actors in order to strengthen cybersecurity in Europe. Indeed, to counter these growing cyber threats, the EU and its member states

[32] Eleni Kapsokoli, "Sanctions and Cyberspace: The Case of the EU's Cyber Sanctions Regime," *Academic Conferences International Limited* (2021): 492, https://doi.org/10.34190/EWS.21.029
[33] "ENISA Threat Landscape 2022," op. cit.
[34] Martina Calleri, ''The European Union as a Global Actor in Cyberspace: Can the Cyber Sanctions Regime Effectively Deter Cyber-Threats?'' *Romanian Cyber Security Journal* 2, 2 (2020): 4.

developed instruments and policies to fight against cybercrimes, cyberespionage, cyberattacks against infrastructures and hybrid threats using cyber means.[35] As part of its strategy to ensure a more secure cyberspace, the EU emphasises the importance of a secure cyberspace in which fundamental rights and the rule of law are respected.

Hence, as part of its cyber-deterrence strategy, the EU first adopted in February 2013 its EU Cybersecurity Strategy (EUCSS) which aims at ensuring a common level of network information security across the EU.[36] This 2013 EUCSS, consisting of a directive, developed an internal market for cybersecurity products and services and fostering Research and Development investment.[37] Thus, this directive created a cyber internal market in order to strengthen the security and resilience of networks and information systems within the EU. During this same year, the EU also intended to strengthen its relations with regional and international partners, as cyberspace has no tangible borders. The European Cybercrime Centre (EC3) at Europol was established in The Hague which harmonises the cybersecurity capabilities of EU member states to fight against cybercrimes.[38] It also cooperates with international partners with regards investigations of cybercrimes.

Another major pillar of cybersecurity as part of EU's cybersecurity strategy is the 2016 Directive on Security of Network and Information Systems (NIS Directive).[39] It is the first piece of EU cybersecurity legislation which enhances cybersecurity in the EU by setting up national Computer Security Incident Response Teams and a competent national NIS authority. In this continuity, 2017 was an important year because the European Commission launched the Cybersecurity Package. Among the provisions, the most notable remains the permanent mandate granted the EU Agency for Network and Information Security (ENISA) which mainly ensures the implementation of the NIS Directive.

Cybersecurity has become such a priority for the EU that even a cyber diplomacy has been developed within the framework of the CFSP. Indeed, the increase of state-sponsored cyberoperations and cyberattacks, stemming mostly from Russia, China, Turkey, Iran and

---

[35] Paul Ivan, "Responding to cyberattacks: Prospects for the EU Cyber Diplomacy Toolbox," Discussion Paper, *Europe in the world programme* (2019): 4, http://aei.pitt.edu/97071/1/pub_9081_responding_cyberattacks.pdf
[36] Simon Shooter, "Cyber Security and the EU: regulating for network security," *Bird& Bird* (2013): 1.
[37] Ibid.
[38] "The Development of the EU Cyber Security Strategy and its Importance," Jorida Vela, FINABEL, accessed 3 November 2022, https://finabel.org/info-flash-the-development-of-the-eu-cyber-security-strategy-and-its-importance/
[39] "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union," European Parliament and Council of the European Union, OJ L 194, 19 July 2016, http://data.europa.eu/eli/dir/2016/1148/oj

North Korea, has raised awareness of the political importance and international challenges laid behind cybersecurity.[40] Therefore, progressively the EU institutions have contributed to international cybersecurity by developing the so-called Cyber Diplomacy Toolbox 2017.

The development of the Cyber Diplomacy Toolbox started in 2015. As a matter of fact, the Council of the EU claimed that in order to effectively reduce the risks of cyber threats, it is necessary to make use of all the legal and diplomatic instruments available to the EU.[41] These conclusions recognise that the mitigation of cyberattacks and conflict prevention entail both a legal and diplomatic response. So, the concrete idea of developing a "joint EU diplomatic response against coercive cyber operation" emerged by the Dutch presidency of the Council in 2016.[42] This document sets the first steps towards an EU cyber diplomacy shifting from the traditional EU cybersecurity strategy. From that moment on, the dice are cast and the development of the Cyber Diplomacy Toolbox became a reality.

On March 2017, both the European External Action Service (EEAS) and the European Commission presented a joint issues paper on a joint EU diplomatic response to cyber operations.[43] This paper was later examined by the Horizontal Working Party on Cyber Issues which is responsible for coordinating the Council's work on cyber issues (mainly the cyber policy and legislative activities). Thus, a joint EU diplomatic response seeks to impose efficient consequences on perpetrators of cyberattacks to ensure a safer cyberspace. On 19 June 2017, the Council of the EU adopted the draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox").[44] This Cyber Diplomacy Toolbox is part of EU's cyber diplomacy strategy within the CFSP. According to the Council in its conclusions, there is a symbolic need to use the all CFSP instruments and measures to counter both state and non-state actors who are behind cyber-malicious activities.[45] It is necessary for the EU to ensure the protection and the security of its member states and its citizens against cyberattacks. Hence, the Cyber Diplomacy Toolbox

[40] Ivan, op. cit., 5.
[41] "Draft Council conclusions on Cyber Diplomacy," Council of the European Union, OJ 6122/15, 11 February 2015, https://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf
[42] "Non-Paper: Developing a Joint EU Diplomatic Response Against Coercive Cyber Operations," Council of the European Union, 5797/6/16, 19 May 2016, http://statewatch.org/news/2016/jul/eu-council-diplomatic-response-cyber-ops-5797-6-16.pdf

[43] Annegret Bendiek, "The European Union's Foreign Policy Toolbox in International Cyber Diplomacy," *Cyber, Intelligence, and Security* 2, 3 (2018): 62.
[44] "Council conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")," Council of the European Union, OJ 10474/17, 19 June 2017, https://data.consilium.europa.eu/doc/document/ST-10474-2017-INIT/en/pdf
[45] Ibid.

encourages cooperation, facilitate mitigation of immediate and long-term threats, and influence the behaviour of potential long-term aggressors.[46]

On 11 October 2017, the implementing guidelines for the Cyber Diplomacy Toolbox were approved by the Political and Security Committee.[47] The latter refers to five categories of measures within the CFSP that can be used against cyber malicious acts directed against the EU or its members states.[48] Notably, the Cyber Diplomacy Toolbox includes "restrictive measures" adopted in accordance with the procedure set out in article 29 TEU coupled with article 215 TFEU. Needless to say, this EU diplomatic response to cyberattacks shall be proportionate to the scope, scale, duration, intensity, complexity, sophistication and impact of each cyber activity.[49] Moreover, the CFSP measures within the Cyber Diplomacy Toolbox shall undeniably respect international law and fundamental rights.

On 16 April 2018, the Council adopted conclusions on malicious cyber activities, in which it stressed the importance of an open, free, secure and stable global cyberspace and expressed its concerns about the activities of malicious actors.[50] Here, the Council stated that the EU upholds the international consensus that existing international law is applicable to cyberspace and emphasised that respect for international law, especially from the United Nations Charter, is essential to maintaining peace and stability.[51] What is all the more striking in these conclusions is the formal condemnation by the EU of the attacks of WannaCry and NotPetya. Indeed, the EU condemned the malicious use of information and communications technologies in these attacks which have cause disastrous and significant economic damages in the EU.[52] The EU emphasised that the misuse of ICTs is totally contrary to EU values and the rule of law as it undermines the security and safety of the cyberspace. In this official condemnation initiative, the High Representative, Federica Mogherini declared on 12 April 2019 malicious cyber activities, including intellectual property theft would not be tolerated and

[46] Ibid.
[47] "Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities," op. cit.
[48] Ibid.
[49] Ibid.
[50] "Council conclusions on malicious cyber activities," Council of the European Union, OJ 7925/18, 16 April 2018, http://data.consilium.europa.eu/doc/document/ST-7925-2018-INIT/en/pdf
[51] Ibid.
[52] Ibid.

called on all partners to strengthen international cooperation to promote security and stability in cyberspace.[53]

Therefore, this led the European Council called for further work on the capacity to respond to and deter cyber-attacks on October 2018. In this context of EU's resilience, deterrence and response to cyber-attacks, the Council of the EU adopted on 17 May 2019 a framework for targeted restrictive measures to deter and respond to cyber-attacks with a significant effect which constitute an external threat to the Union or its Member States, including cyber-attacks against third countries or international organisations where restrictive measures are deemed necessary to achieve CFSP objectives.[54] In particular, this framework allows the EU for the first time to impose sanctions on persons or entities responsible for, or involved in, cyberattacks. These restrictive measures include travel bans, freezing of assets and the prohibition of making funds.

This autonomous sanctions regime against cyber-malicious actors demonstrates the needed and symbolic action of the EU in its cyber-resilient strategy. This cyber sanctions regime is a significant step for the EU in operational terms. It also shows its concern and political commitment in building a cyber resilience and ensuring a safe and secure cyberspace within the EU.

A key date remains 30 July 2020 when the EU imposes its first ever sanctions against six persons and three entities responsible for or involved in various cyber-attacks. A second package of cyber sanctions was imposed on 22 October 2020. Since these two impositions of sanctions in response to cyberattacks, the cyber sanctions regime has not been used. Yet, the 17 May 2019 framework of restrictive measures against cyberattacks remains relevant. Indeed, the application of the sanctions regime is reviewed by the Council every year and has been extended twice. First extended until May 2021, the Council decided to extend the cyber sanctions regime for three further years.[55] Thus, currently, the framework for restrictive measures against cyber-attacks is effective until 18 May 2025.[56] Therefore, currently the cyber sanctions regime still applies. This demonstrates EU's strong deterrence and resilience will to respond to malicious cyber acts so as to protect EU's and its member states' security and interests.

---

[53] "Declaration by the High Representative on behalf of the EU on respect for the rules-based order in cyberspace," Council of the European Union, *Press release*, 12 April 2019, https://europa.eu/!rm83yB
[54] "Cyber-attacks: Council is now able to impose sanctions," op. cit.
[55] "Extension of cyber sanctions regime to 18 May 2025," Council of the European Union, *Press release*, 16 May 2022, https://europa.eu/!qfDkPr
[56] Ibid.

These different EU institutional initiatives against cyber malicious acts demonstrate EU's concern about the risks for our democracy laid behind cyberthreats. Obviously, cybersecurity, as currently bringing new and evolving legal challenges, remains a priority for the EU; this is reflected by the next long-term budget (2021-2027) in supporting digital technologies.[57] Therefore, the EU decided to respond diplomatically within the CFSP through the adoption of its Cyber Diplomacy Toolbox; it demonstrates the EU's resilient approach to cyber-attacks (1.1.2.).

1.2. The Cyber Diplomacy Toolbox, a resilience instrument in the spirit of the CFSP

The growth and increase of cyber malicious acts forced the EU to develop appropriate diplomatic means to find an effective response beyond other EU cybersecurity policies.

As part of the EU diplomacy strategy, the Cyber Diplomacy Toolbox was developed by EU institutions within its CFSP. Indeed, the EU expressed its concerns in view of the new risks posed by cyber threats. The EU's external policies, in particular the CFSP, are not immune to the challenges posed by cyber threats. As a matter of fact, cyber malicious acts perpetrated by either state or non-state actors are constantly rising. This increase is reflected both in the intensity of cyber-attacks and in their impact or sophistication.

This phenomenon demonstrates the progressive change that our societies are experiencing. Notably, scholars and analysts have observed the shift from traditional warfare to cyberwarfare. As early as 2014, Cirlig already pointed out the fact that cyber warfare will constitute a new type of warfare that will constitute an important and strategic support to traditional military tactics.[58] This new shift of conflict has been analysed through the statement of the former French Minister of Armed Forces, Florence Parly. In 2019, she stated, alongside its new French Military Cyber Strategy, that "cyber warfare has begun and France must be ready to fight it"[59]. Thus, cyberattacks are becoming a new tool for warfare.

[57] "The Development of the EU Cyber Security Strategy and its Importance," op. cit.
[58] Carmen-Cristina Cirlig, "Cyber defence in the EU. Preparing for cyber warfare?" *European Parliamentary Research Service* PE 542.143 (2014): 2.
[59] ''Déclaration de Madame, ministre des armées, sur la stratégie cyber des armées,'' Paris, January 18, 2019, accessed 4 October 2022, https://www.vie-publique.fr/discours/269137-florence-parly-18012019-strategie-cyber-des-armees-cyberdefense

Subsequently, the EU needed to develop diplomatic instruments, within its CFSP, to ensure the adequate and sufficient level of protection for its institutions, member states and citizens against cyber threats. Therefore, the EU affirms its commitment to the resolution of international disputes in cyberspace by peaceful means.[60] The EU upholds the applicability of international legislation and principles to cyberspace, especially stemming from the Budapest Convention or the reports of the United Nations Groups of Governmental Experts.[61] It follows that EU diplomacy strategy and approach should focus on ensuring security and stability in cyberspace through enhanced international cooperation. Hence, the EU's cyber diplomacy is part of its deterrence and resilience strategy which consists of dissuading perpetrators of malicious cyber acts by signalling them that their illegal actions will have consequences.[62] Hence, the Cyber Diplomacy Toolbox was developed and adopted in 2017 as part of the CFSP so as to respond to cyberattacks. The Cyber Diplomacy Toolbox follows the EU's resilience and deterrence strategy which provides CFSP instruments to secure the cyberspace in the EU rather than creating a coercive international law mechanism holding third states responsible for cyberattacks.[63]

In the context of an effective CFSP response, the Cyber Diplomacy Toolbox defines a common EU diplomatic response to cyber-attacks in the event of a cyberattacks targeting the Union.[64] This framework specifies all the CFSP measures to reinforce the security within the EU, for its member states and citizens. The Cyber Diplomacy Toolbox can be used to contribute to conflict prevention, the mitigation of cybersecurity threats, and greater stability in international relations.[65] The framework should encourage cooperation, facilitate mitigation of immediate and long-term threats, and influence the behaviour of potential long-term aggressors.[66] Moreover, the framework for an EU diplomatic response to cyberattacks shall be

[60] "Council conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")," op. cit.
[61] Ibid.
[62] Joseph S. Nye, "Deterrence and Dissuasion in Cyberspace," *International Security* 41, 3 (2017): 45, https://doi.org/10.1162/ISEC_a_00266
[63] ''Si vis cyber pacem, para sanctiones: the EU Cyber Diplomacy Toolbox in action,'' Samuele De Tomas Colatin, NATO Cooperative Cyber Defence Centre of Excellence, accessed 4 October 2022, https://ccdcoe.org/library/publications/si-vis-cyber-pacem-para-sanctiones-the-eu-cyber-diplomacy-toolbox-in-action/
[64] "Council conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")," op. cit.
[65] Ibid.
[66] Ibid.

proportionate to the scope, scale, duration, intensity, complexity, sophistication and impact of each cyber activity.[67]

It appears from the Cyber Diplomacy Toolbox that its primary and main goal, following the deterrence approach, is to mitigate cyber threats and influence the behaviour of potential perpetrators of malicious cyber acts. Yet, for it to be an CFSP efficient instrument, it shall be complementary to existing cybersecurity policies, notably the NIS Directive, the activities of ENISA and the EC3 at Europol.[68] Indeed, for the Cyber Diplomacy Toolbox to be effective, it cannot replace the existing EU cyber diplomacy efforts.

Thus, the Cyber Diplomacy Toolbox shall ensure the protection, integrity and security of the EU, its Member States and their citizens. In order to reach such an objective, this diplomatic response is based on suitable measures within the CFSP that shall respect the values of the EU, and most importantly the rule of law. Indeed, the measures provided by the Cyber Diplomacy Toolbox shall respect applicable international law and fundamental rights.[69] Moreover, the Cyber Diplomacy Toolbox shall be in line with the CFSP objectives as set out in article 21 of the Treaty on the European Union (TEU).[70] That means that the measures provided by the Cyber Diplomacy Toolbox shall ensure mainly the safeguarding of EU's values, fundamental interests, security, independence and integrity; the consolidation and support of democracy, the rule of law, human rights and the principles of international law; and the preserving of peace, prevention of conflicts and strengthening of international security.[71]

In view of the significant risks posed by cyber threats and cyber-attacks, it has become necessary for the EU to ensure an efficient response by the trigger of CFSP measures that the Cyber Diplomacy Toolbox provides for. This diplomatic response is based on a gradation of five CFSP measures ranging from simple diplomatic cooperation and dialogue to preventive measures against cyber-attacks and sanctions.[72]

---

[67] Ibid.
[68] "Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities," op. cit.
[69] Ibid.
[70] Ibid.
[71] "Consolidated Version of the Treaty on The Functioning of the European Union signed on 13 December 2007," OJ C 326/47, 26 October 2012, article 21, paragraph 2, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2008:115:0013:0045:en:PDF
[72] Brunessen Bertrand,"La souveraineté numérique européenne : une « pensée en acte » ?," *Revue Trimestrielle Droit Européen* 2 (2021): 262, https://www.dalloz.fr/documentation/Document?id=RTDEUR/CHRON/2021/0394

The implementing guidelines of the Cyber Diplomacy Toolbox refer and explain the five diplomatic measures the EU and Member states can undertake, including preventive measures, cooperative measures, stability measures, restrictive measures and supportive measures within the CFSP. All these measures, which are an integral part of the Cyber Diplomacy Toolbox, have the common objective of signalling and responding to malicious cyber activities. They all, with more or less consequences, aim at influencing the behaviours of cyber attackers and mitigating cyber threats. Therefore, in compliance with EU's values, the abovementioned measures serve to protect and ensure the security of its member states and citizens. This is why the effectiveness of the Cyber Diplomacy Toolbox requires the use of all these measures either independently or in coordination.

The most remarkable and striking instrument in the EU's cyber diplomatic strategy is the restrictive measures. They refer to sanctions as part of the CFSP.[73] They shall be imposed following the two-step approach required by EU Treaties. First on the basis of a Council Decision adopted under article 29 TEU, then a Council Regulation adopted under article 215 TFEU. Thus, when it comes to cyber deterrence, the EU may impose sanctions in response to malicious cyber acts, if deemed necessary. Respecting the principle of proportionality, restrictive measures include travel bans, arms embargoes and freezing funds or economic resources.

With regards to the objective that Cyber Diplomacy Toolbox aims to achieve, it is evident that it corresponds to an CFSP instrument of resilience to the growing increase of cyber threats in cyberspace within the EU. This resilience approach is explained by the diplomatic strategy adopted by the EU, which is merely a materialization of its strong commitment to cyber deterrence. This EU cyber deterrence strategy has been demonstrated through other EU initiatives over the past ten years. Indeed, the EU institutions responded against these growing challenges that cyber threats brought to EU's security, economy and democracy. In particular through policies such as the 2013 EU Cybersecurity Strategy and the 2016 NIS Directive, or agencies such as the EC3 and ENISA. The EU aims at strengthening its resilience in cyberspace and protecting human rights of its citizens. Obviously, the Cyber Diplomacy Toolbox of 2017 constitutes the culminated diplomatic instrument in compliance with EU's cyber deterrence strategy. This latter strategy was strengthened with the formal introduction of a cyber sanctions regime in 2019 (part 2).

[73] Ibid.

2. The new EU cyber sanctions regime

This new EU cyber sanctions regime has been introduced following the traditional two-step approach stemming from article 29 TEU and article 215 TFEU. As a matter of fact, the new legal framework for restrictive measures targeting those responsible for cyberattacks was implemented with the adoption of Decision (CFSP) 2019/797 – based on article 29 TEU – and Regulation (EU) 2019/796 – based on article 215 TFEU (2.1.). This new cyber sanctions regime has been used by the EU twice since its adoption. The EU first imposed cyber sanctions on 30 July 2020; the second time on 22 October 2020. These are the two current and only cyber sanctions packages the EU has imposed up until now (2.2.).

2.1. The adoption of restrictive measures against cyber-attacks: Decision (CFSP) 2019/797 and Regulation (EU) 2019/796

The Cyber Diplomacy Toolbox introduced in 2017 constitutes a symbolic CFSP instrument with regards to the EU's resilience and deterrence strategy to respond against cyber malicious acts. Thus, according to the Cyber Diplomacy Toolbox and its implementing guidelines, the restrictive measures against cyber malicious acts can be imposed following the traditional two-step approach (2.1.1.). Undeniably, as being *per se* CFSP instruments, the restrictive measures against cyber-attacks must respect the objectives as laid down in article 21 TEU (2.1.2.). This new cyber sanctions regime is part of the four current autonomous and horizontal sanctions regime adopted by the EU (2.1.3).

2.1.1. The traditional two-step procedure: article 29 TEU and article 215 TFEU

According to the Cyber Diplomacy Toolbox and its implementing guidelines, the restrictive measures against cyber malicious acts can be imposed following the traditional two-step approach.[74] In other words, the EU cyber sanctions regime follows the normal EU procedures to adopt an autonomous sanctions regime in compliance with two articles from the EU Treaties. Namely, the coupling of article 29 TEU and article 215 TFEU. First, on the basis of article 29 TEU, the adoption by the Council of a CFSP decision laying down the overall sanctions framework. Second, on the basis of article 215 TFEU, the latter is accompanied by

[74] Miadzvetskaya, op. cit., 280.

the associated EU Regulation. Thereby, this coupling of article 29 TEU and article 215 TFEU introduces an autonomous EU sanctions regime.

Thus, in the context of EU's CFSP, restrictive measures are adopted following the two-step approach. First, article 29 TEU allows the Council of the EU to adopt a decision to impose sanctions against non-EU countries, non-state entities and individuals.[75] As being a CFSP decision, it is subject to the decision-making rules governing EU's CFSP. On the basis of proposals from the High Representative of the Union for Foreign Affairs and Security Policy, the Council has to agree on unanimity on the decision to impose sanctions; each member state has the right of veto. This CFSP decision consists of a pre-condition to the imposition of sanctions; it sets out the overall framework of the restrictive measures. Second, according to article 215 TFEU, the Council may adopt the necessary measures to implement the CFSP decision adopted under article 29 TEU to ensure its uniform application throughout its member states. As an ordinary EU implementing legal act, it follows the normal EU procedures. Thus, on a joint proposal from the High Representative and the Commission, the Council may adopt either a Regulation or a Decision acting by a qualified majority.[76] The European Parliament shall be informed by the Council to exercise democratic scrutiny on the EU's external action and ensure that the Council did not abuse of its prerogatives.[77]

On 17 May 2019, the EU established the new cyber sanctions regime allowing the EU, for the first time, to impose sanctions on persons or entities responsible for, or involved in, cyber-attacks. The cyber sanctions regime stems from two decisions adopted by the Council following this exact EU procedure. Indeed, the Council first adopted at unanimity Decision 2019/797 on the basis of article 29 TEU.[78] Then, to implement this decision, the Council adopted by qualified majority Regulation 2019/796 on the basis of article 215 TFEU.[79]

Nevertheless, the adoption of such a regime has not been confronted without difficulty. As a matter of fact, Italy was firmly opposed to the idea and introduction of a new cyber

[75] "Consolidated Version of the Treaty on European Union signed on 13 December 2007," op. cit., article 29.
[76] "Consolidated Version of the Treaty on The Functioning of the European Union signed on 13 December 2007," op. cit., article 215, paragraph 1.
[77] Ibid.
[78] "Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States," Council of the European Union, OJ L 129I, 17 May 2019, http://data.europa.eu/eli/dec/2019/797/oj
[79] "Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States," Council of the European Union, OJ L 129I, 17 May 2019, http://data.europa.eu/eli/reg/2019/796/oj

sanctions regime.[80] In a less firm manner, Belgium, Finland and Sweden promoted for a "*gradual response*" to future cyberattacks where sanctions would be a last resort instrument.[81] Yet, some member states were strongly in favour of the adoption of such a sanctions regime, especially the United Kingdom, France, Estonia, the Netherlands, Romania, Slovakia, Latvia, Lithuania and Poland.[82] Therefore, reaching unanimity to adopt the decision setting the overall framework of the cyber sanctions regime was not an easy task. Yet, after long discussions among the Council, the member states succeeded in adopting the new cyber sanctions regime. This regime all the more became a success as it has had impact on neighbour countries. Indeed, North Macedonia, Montenegro, Albania, Bosnia and Herzegovina, Iceland, Norway and Ukraine aligned their national law with the Council Decision 2019/797.[83] This demonstrates EU's strong will and commitment in cyber deterrence which fortunately has an impact on third states.

Ultimately, Council Decision 2019/797 and Council Regulation 2019/796 establish the legal framework which allows the EU to impose sanctions to deter and respond to cyber-attacks, which constitute an external threat to the EU or its Member States. This cyber sanctions regime corresponds to a new and suitable CFSP tool aiming at reaching the Cyber Diplomacy Toolbox's purpose; namely to mitigate cyber threats and influence the behaviours of perpetrators of cyberattacks in the long term.

2.1.2. The consistency with CFSP objectives stemming from article 21 TEU

In the past few years, restrictive measures have become an essential tool in the CFSP to respond to major geopolitical challenges.[84] Indeed, as the EU lacks a common EU military defence, the EU sanctions have become a necessary and powerful CFSP tool. Thus, CFSP sanctions constitute a coercive diplomatic tool through which the EU may exert pressure on third countries, individuals or companies. Nevertheless, EU sanctions are not punitive nor vindicative measures. They aim at reaching a certain objective set out by the sanctions'

[80] "Italy resisting EU push to impose sanctions over cyberattacks,"Guarascio Francesco, Reuters, accessed 10 November 2022, https://www.reuters.com/article/us-italy-russia-sanctions-idUSKCN1MM2CP
[81] Miadzvetskaya, op. cit., 286.
[82] Ibid.
[83] "Declaration by the High Representative on behalf of the EU on the alignment of certain countries concerning restrictive measures against cyber-attacks threatening the Union or its Member States," Council of the European Union, *Press release*, 7 June 2022, https://europa.eu/!MBbph7
[84] "Frequently asked questions: Restrictive measures (sanctions)," European Commission, 26 February 2022, accessed 9 November 2022, https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_1401

framework. In other words, by targeting specific entities or individuals responsible for the malicious behaviour, restrictive measures shall encourage the required change in policy or activity and do not have an economic motivation.[85] Therefore, when adopting sanctions, the EU must ensure they follow and respect the CFSP goals as provided by article 21 TEU. That means that restrictive measures, as being one of the various CFSP instruments, must reach and be guided by the following objectives. First, to safeguard EU's values, fundamental interests, and security.[86] Second, to preserve peace, prevent conflicts and strengthen international security in accordance with the principles of the UN Charter.[87] Third, to consolidate and support democracy, the rule of law, human rights, and the principles of international law.[88] Consequently, EU sanctions must always be consistent with CFSP objectives as laid down in article 21 TEU.

As part of the CFSP, restrictive measures represent one of various instruments at the EU's disposal so as to prevent conflicts or respond to political crises. As non-punitive instruments, they aim at reaching the principles of the EU's external policy laid down under article 21 TEU. Namely they are preventive and anticipative measures. The cyber sanctions regime was adopted in consistency with these objectives provided by article 21 TEU.

As a matter of fact, the cyber sanctions regime aims at ensuring cyber security against threats of cyber nature. It seeks to build and ensure an open, global, free, peaceful and secure cyberspace in the EU. The cyber sanctions regime shall support the rule of law as well as fundamental rights, notably the right to privacy and freedom of expression. Moreover, the cyber sanctions regime contributes to conflict prevention, the mitigation of cybersecurity threats, and greater stability in international relations. Thus, it seeks at maintaining peace and stability in cyberspace by respecting international law and the UN Charter.[89] Therefore, the cyber sanctions regime was adopted in compliance with the CFSP objectives as laid down in article 21 TEU, notably to preserve peace, prevent conflicts and strengthen international security in accordance with the principles of the UN Charter.[90]

[85] Ibid.
[86] "Consolidated Version of the Treaty on European Union signed on 13 December 2007," op. cit., article 21, paragraph 2, sub-paragraph a.
[87] Ibid., article 21, paragraph 2, sub-paragraph c.
[88] Ibid., article 21, paragraph 2, sub-paragraph b.
[89] "Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States,". op. cit.
[90] "Consolidated Version of the Treaty on European Union signed on 13 December 2007," op. cit., article 21, paragraph 2, sub-paragraph c.

As some of the EU's interests are linked to the stability of its partners countries, the regime is applicable in response to cyber-attacks with a significant effect against third states or international organisations.[91] Indeed, this cyber sanction regime is part of EU's CFSP, so in that case the regime can be imposed only if it deemed necessary to achieve CFSP objectives as laid down under article 21 TEU; notably to maintain international peace and security and to support human rights, the rule of law and the international principles of law.

2.1.3. A decentralised and horizontal cyber sanctions regime

With regards to the adoption of sanctions for the EU, the EU has actually two options. In other words, there is a traditional division when it comes to the adoption of sanctions. Either the EU can adopt sanctions based on a United Nations Security Council resolution; i.e., a centralised sanction. Or the EU can adopt its own sanctions according to the procedures laid down in the EU treaties; i.e., decentralised sanctions.

As far as decentralised sanctions are concerned, the Lisbon Treaty brought the last evolution with its article 215 TFEU. Article 215 TFEU distinguishes sanctions adopted against third countries in paragraph 1 (especially embargoes against third states) and sanctions adopted against individuals in paragraph 2 (also known as smart sanctions or targeted sanctions). Nowadays, EU sanctions typically target military or political elites, most commonly in the form of visa bans, asset freeze and arm embargoes.

The new EU cyber sanctions regime is an autonomous and decentralised sanctions regime. Indeed, the legal framework for restrictive measures against cyber-attacks stems from two decisions adopted by the Council: Council Decision 2019/797 and Council Regulation 2019/796 from 17 May 2019. These two decisions did not implement any UN Security Council Regulation, rather followed the two-step procedure. This decentralised sanctions regime has the advantage of allowing the Council to act promptly and immediately. Indeed, by being autonomous, the Council only needs to update the annexed listings of targeted persons instead of adopting a completely new legal framework each time a new sanction has to be imposed.[92]

[91] "Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States,". op. cit., article 1, paragraph 6.; and "Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States," op. cit., article 1, paragraph 6.

[92] Yuliya Miadzvetskaya, and Ramses A. Wessel, ''The Externalisation of the EU's Cybersecurity Regime: The Cyber Diplomacy Toolbox,'' *European Paper* 7, 1 (2022): 430, https://ssrn.com/abstract=4199627

In the recent years, the EU has developed more and more autonomous and decentralised sanctions regimes. Surprisingly, among forty-six EU sanctions regimes in place in 2022, only four are horizontal in nature.[93] Conversely to country specific regimes, horizontal sanctions regimes are thematic regimes that target specific persons or entities responsible for activities that breach a specific norm. These four horizontal sanctions regimes include sanctions addressing the use of chemical weapons, the EU's terrorist list, the cyber sanctions regime and the Magnitsky-type Act.[94] The European Magnitsky Act constitutes EU's main evolution in sanction regime in respect for *erga omens* and Human Rights.[95] It is a horizontal (non-country specific) mechanism for sanctioning gross human rights abuses.

The cyber sanctions regime is horizontal sanctions regime. Indeed, it is a themed sanctions regime that follows the targeted approach. The cyber sanctions regime targets individuals or entities responsible for cyberattacks with the adoption of Decision (CFSP) 2019/797 and Regulation (EU) 2019/796. As part of the EU's CFSP, this new cyber sanctions regime consists of a diplomatic response to cyberattacks. With the Cyber Diplomacy Toolbox, the EU confirms a move towards diversification of thematic regimes of restrictive measures.[96]

Following the establishment of the cyber sanctions regime through Decision 2019/797 and Regulation 2019/796, the Council adopted two packages of cyber sanctions in 2020 against cyber-attacks that had threated the EU and its member states (2.2.).

2.2. The two current and only restrictive measures against cyber-attacks threatening the Union or its Member States

Since the establishment of the cyber sanctions regime through the Decision 2019/797 and Regulation 2019/796, the EU has imposed sanctions only twice. As a matter of fact, the EU imposed two packages of sanctions against persons and entities responsible for cyberattacks causing disastrous damages to the EU and its member states: one on 30 July 2020 and one on

[93] Ibid. 431.
[94] Ibid.
[95] "Council Decision (CFSP) 2020/1999 of 7 December 2020 concerning restrictive measures against serious human rights violations and abuses," Council of the European Union, OJ L 410I, 7 December 2020, http://data.europa.eu/eli/dec/2020/1999/oj
[96] Louis-Marie Chauvel, and Anne Hamonis, ''Chronique Action extérieure de l'UE. La diversification des régimes thématiques de mesures restrictives,'' *Revue Trimestrielle Droit Européen* 3 (2019): 746, https://www.dalloz.fr/documentation/Document?id=RTDEUR/CHRON/2019/0631

22 October 2020. These are the two current and only cyber sanctions packages the EU has imposed since the adoption of the cyber sanctions regime.

Thus, at the current state, eight persons and four entities are targeted by cyber restrictive measures.[97] They were found responsible for disastrous major cyber-attacks, namely WannaCry, NotPetya, Operation Cloud Hopper, the attempted cyberattack against the Organisation for the Prohibition of Chemical Weapons (OPCW) and the Bundestag Hack. These sanctions show the EU's resilience will to prevent, discourage, deter and resist to cyber-attacks.[98]

Interestingly, this cyber sanctions regime provides for targeted sanctions only. That means that they are only directed at individuals and entities found responsible for the cyber-attacks.[99] So, for the sanction to be proportional in response for the behaviour of the cyber-attacker, it requires to go through the preliminary step which is attribution. For the EU to adopt a cyber sanction, it is necessary to undergo the whole attribution process, which will be analysed further in the second part. The legal attribution requires the EU to classify the cyber-attacks. That means to assess whether the criteria for enlisting a person found responsible for a cyber-attack as defined by Decision 2019/797 and Regulation 2019/796 are met.

Needless to say, in order to ensure the establishment of the cyber sanctions regime, the analysis of the criteria for imposing a sanction is necessary. Both Decision 2019/79 and Regulation 2019/796 provide the necessary explanations for the types of measures (2.2.1.), the subjects (2.2.2.), the scope (2.2.3.) and the grounds for the listing (2.2.4.) of this newly established regime.

2.2.1. Types of restrictive measures

Generally, restrictive measures include prohibitions on the export of arms and related equipment; restrictions on admission on the EU territory (visa or travel bans); economic measures such as restrictions on imports and exports; freezing of funds and economic resources owned or controlled by targeted individuals or entities. In certain cases, exceptions from the

[97] "Extension of cyber sanctions regime to 18 May 2025," op. cit.
[98] Ibid.
[99] Miadzvetskaya, and Wessel op. cit., 429.

asset freeze may be granted to allow the export of products to meet basic needs, such as food or medicines.

The horizontal cyber sanctions regime consists of traditional and conventional restrictive measures. Namely, these restrictive measures include bans on persons travelling to the EU and asset freezing.

As a matter of fact, article 4 of Decision 2019/797 provides for the travel bans taken by Member States against perpetrators of cyber-attacks. The Member States may still be able to grant an exemption to the travel ban. It details the conditions under which such an exemption can be granted; especially if justified on grounds of urgent humanitarian needs.[100]

Moreover, article 5 of Decision 2019/797 and article 3 of Regulation 2019/796 provide for the freezing of all funds and economic resources owned, held or controlled by persons responsible for cyber-attacks.[101] Obviously, both the Decision and the Regulation detail the derogations under which the member states are authorised the release of certain frozen assets and funds.

2.2.2. Subjects of the restrictive measures

The cyber sanctions regime follows the EU smart and targeted approach; they are not broad economic sanctions. Indeed, these sanctions are directed at the individuals and entities responsible for the attacks from a perspective of their behaviour, not against third states.[102]

According to article 4 of the Decision 2019/797 and article 3 of the Regulation 2019/796, the EU may impose sanctions against natural of legal persons, entities or bodies responsible for cyber-attacks or attempted cyber-attacks; who provide financial, technical or material support for such attacks or who are involved in other ways. [103] Sanctions may also be imposed on persons or entities associated with them.[104] Thus, the names of the natural or legal,

[100] "Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States,". op. cit. article 4, paragraphs 5, 6, and 7.
[101] "Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States,". op. cit., article 5, paragraphs 1 and 2.; and "Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States," op. cit., article 3.
[102] Miadzvetskaya, and Wessel op. cit., 429.
[103] "Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States,". op. cit., article 4, paragraph 1.; and "Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States," op. cit., article 3, paragraph 3.
[104] Ibid.

entities and/or bodies targeted by the sanctions will be annexed to these abovementioned Decision and Regulation.

For instance, on 30 July 2020, the EU imposed for the first-time cyber sanctions. Indeed, the Council unanimously adopted restrictive measures with travel bans and asset freezes against six individuals and three entities (Chinese, North-Korean and Russian) that have been found responsible for or involved in various cyber-attacks against EU Member States.[105] The targeted persons and entities are responsible for the following malicious cyber-attacks: WannaCry, NotPetya, Operation Cloud Hopper and the attempted cyberattack against the OPCW.

Moreover, on 22 October 2020, the EU imposed cyber sanctions for the second time. Indeed, the Council adopted restrictive measures against two Russian individuals and the GRU that were responsible for or took part in the cyber-attack on the German Federal Parliament (Deutscher Bundestag) in April and May 2015, known as the Bundestag Hack.[106]

Evidently, the fact the EU attributed the abovementioned cyber-attacks to Chinese, North Korean and Russian individuals and entities represents a brave response in terms of cyber diplomacy.[107] Indeed, while the US, the UK, Australia and Canada publicly supported this policy initiative, Russia and China criticized the EU for imposing sanctions instead of using a lesser a diplomatic tool like the dialogue.[108] Nevertheless, the legal framework for cyber sanctions regime stemming from Decision 2019/797 states clearly that these restrictive measures are targeting natural and legal persons only.[109] Thus, they are to be distinguished from the attribution of responsibility for cyber-attacks to a third state, which remains a sovereign political decision based on all-source intelligence.[110] Yet, although cyber sanctions are aimed at targeting individuals and entities responsible for cyber-attacks only, the delimitation between targeted sanctions and attribution of responsibility if a third state is quite superficial.[111] Indeed, in the cyber cold war context, the major cyber-attacks WannaCry and NotPetya were mostly supported by foreign governments, namely North Korea and Russia in this present case.[112]

---

[105] Brunessen Bertrand, ''Chronique Droit européen du numérique. La nouvelle approche de la cybersécurité européenne,'' *Revue Trimestrielle Droit Européen* 1 (2021): 156-157, https://www.dalloz.fr/documentation/Document?id=RTDEUR/CHRON/2021/0112

[106] "EU sanctions two individuals and one body over 2015 Bundestag hack," Council of the European Union, Press release, 22 October 2022, https://europa.eu/!CJ48PC

[107] Kapsokoli, op. cit., 496.

[108] Ibid.

[109] "Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States,". op. cit.

[110] Ibid.

[111] Miadzvetskaya, and Wessel op. cit., 435.

[112] Ibid.

Thus, although the Cyber Diplomacy Toolbox, providing for cyber restrictive measures, seeks to ensure a stable, peaceful and secure cyberspace in the EU, it seems that it also tends to offer an indirect punitive international law mechanism holding third states responsible for cyber-attacks.

2.2.3. Scope of cyber malicious activities

First and foremost, according to article 1 of the Decision and the Regulation, the legal framework for restrictive measures applies to *cyber-attacks with a significant effect*, including *attempted* cyber-attacks with a potentially significant effect, which constitute *an external threat to the Union or its Member States*.[113] From this scope defined by the cyber sanctions regime, three main words and expressions of words are important to be addressed and analysed. First, what the EU means by "*cyber-attacks*" (1.1.1.3.1.) and "*attempted cyber-attacks*" (1.1.1.3.2.) for the purpose of this sanction regime. Second, what does "*significant effect*" inquire in relation to a cyber-attack (1.1.1.3.3.). Finally, in what way is a cyber-attack considered to constitute an "*external threat*" to the EU or its member states (1.1.1.3.4.).

2.2.3.1. Cyber-attack

The main and principal notion is a "cyber-attack". Article 1 of both the Decision and the Regulation defines what the EU understands by a cyber-attack. This definition of cyber-attack is unique and autonomous to the EU. It has been adopted specifically for the purpose of the cyber sanctions regime.[114] It ensures uniformity of interpretation on the notion of cyber-attack between EU's member states.

In compliance with the cyber sanctions regime, a cyber-attack refers to an action involving any of the following: (a) access to information systems; (b) information system interference; (c) data interference; or (d) data interception, where such actions are not duly authorised by the owner or by another right holder of the system or data or part of it, or are not permitted under the law of the Union or of the Member State concerned.[115] In other words,

[113] "Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States,". op. cit., article 1, paragraph 1.; and "Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States," op. cit., article 1.
[114] Pawlak, and Biersteker, op. cit., 66.
[115] "Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States,". op. cit., article 1, paragraph 3; and "Council Regulation (EU)

cyber-attacks are unauthorised actions involving access to and interference with information systems, data interference or data interception.

The fact remains that the new cyber sanctions regime is part of a cyber cold war context, in which cyber-attacks have an undeniable offensive role.[116] Actually, unlike other EU sanctions regime, this is a difficulty specific to the notion of cyber-attacks. Cyber-attacks are very distinct due to intrinsic features of cyberspace such as internet structural design and anonymity.[117] Thus it constitutes an obstacle to the forensic-based attribution to cyber-attackers.[118] Indeed, in the event of a cyber-attack, the cyber defence services struggle to authenticate and designate the attackers due to the electronic paths and signatures used deliberately to blur the tracks.[119] So contrary to other sanctions regime, this criterion for listing represents a challenge for the EU.

2.2.3.2. Attempted cyber-attack

According to article 1 of Decision 2019/797 and Regulation 2019/796, attempted cyber-attacks with a potentially significant effect also fall under the scope of the cyber sanctions regime. Although a potential malicious cyber-attack has not succeeded, it should still be punished. Indeed, the intention of the cyber perpetrator is important to assess the notion of "attempt" regarding a cyber-attack. The reasoning is the following: if the cyber-attack would have been successful, that it would have compromised the security of the network in question, and would have created serious damage to the potential victim, then the perpetrator ought to be held responsible. Of course, this reasoning is held on a case-by-case basis by the Council when adopting a sanction.[120]

However, the difficulty lies with the proof of the potential damage the attempted cyber-attack could cause. There is a challenge in establishing the link between an activity in cyber domain and a potential attempt to cause significant harm.[121] Indeed, it is harder to measure,

2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States," op. cit., article 1, paragraph 3.

[116] Olivier De Maison Rouge, ''L'intégration de contre-mesures économiques dans la prévention des cyberattaques. Le règlement (UE) 2019/796 du 17 mai 2019 et décision (PESC) 2019/797 du 17 mai 2019,'' *Dalloz IP/IT* (2019): 577.

[117] Miadzvetskaya, and Wessel op. cit., 430.

[118] Ibid.

[119] De Maison Rouge, op. cit., 577.

[120] Pawlak, and Biersteker, op. cit., 36.

[121] Ibid.

consequently to prove, the economic impact of a cyber-attack that has not yet terminated.[122] The determination whether the attempted cyber-attack shall fall under the scope of the cyber sanctions regime by listing requires taking into account the broad context of the malicious operation.[123] Of course, a pre-emptive response to attempted cyber-attacks is easily accepted when the EU wants to send a political signal.[124]

For instance, the Council adopted the Decision 2020/1127 of 30 July 2020 in response of, among other, the attempted cyberattack against the OPCW. From a sovereignty perspective, the EU sent a political signal against Russia by targeting four Russian nationals members of the Unit 74455 of Russia's military intelligence agency (GRU). Indeed, these four Russian agents participated in the attempted hacking into the Wi-Fi network of the OPCW in the Netherlands in April 2018.[125] If successful, this cyber-attack would have compromised network security and the ongoing chemical weapons investigation.[126] Here, the agent intended to attack the OPCW by trying to hack into its Wi-Fi network. If the Netherlands Defence Intelligence and Security Service (DISS) had not disrupted the attempted cyber-attack, it would have caused serious damage to the OPCW. Logically, the Council also targeted and enlisted the Main Centre for Special Technologies (GTsST) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU). The involvement of Russian entities and agents in this attempted cyber-attack reinforces the European digital sovereignty challenges of cyber diplomacy.[127]

2.2.3.3. Significant effect

In addition to the notion of cyber-attack, the Decision defines that of "significant effect", which may be only potential. Indeed, in order for the (attempted) cyber-attacks to fall within the scope of the new sanctions regime, they must have a significant impact. The notion of "significant effect" is assessed in the light of a series of alternative defined by the EU in article 3 of Decision 2019/797 and 2 of Regulation 2019/796.[128] A cyber-attack will be considered to have significant effect depending on (a) the scope, scale, impact or severity of disruption

[122] Ibid.
[123] Ibid.
[124] Ibid.
[125] "Council Decision (CFSP) 2020/1127 of 30 July 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States," Council of the European Union, OJ L 246, 30 July 2020, annex, http://data.europa.eu/eli/dec/2020/1127/oj
[126] Ibid.
[127] Bertand, "La souveraineté numérique européenne : une « pensée en acte » ?," op cit., 262.
[128] Chauvel, and Hamonis, op. cit., 746.

caused, including to economic and societal activities, essential services, critical State functions, public order or public safety; (b) the number of natural or legal persons, entities or bodies affected; (c) the number of Member States concerned; (d) the amount of economic loss caused, such as through large-scale theft of funds, economic resources or intellectual property; (e) the economic benefit gained by the perpetrator, for himself or for others; (f) the amount or nature of data stolen or the scale of data breaches; or (g) the nature of commercially sensitive data accessed.[129]

Each criterion will be analysed further alternately.

a) the scope, scale, impact or severity of disruption caused, including to economic and societal activities, essential services, critical State functions, public order or public safety;

It follows from this first criterion that the international principle of state's territorial sovereignty applies to states' activity in cyberspace.

Following the international jurisprudence, in the relations between States, sovereignty signifies independence.[130] It confers to each State the exclusive right to exercise the functions of a State within its territory. As the EU has confirmed that international law applies to cyberspace, consequently does the principle of sovereignty.[131] Thus, the principle of sovereignty applies in relation to states' cyber activities, through the ability of a state to regulate such matters within its territorial borders and to exercise independent state powers.[132]

According to the EU cyber sanctions regime, the violation of a state's territorial sovereignty is assessed in relation to a list of factors stemming from the first criterion. To assess whether a possible violation of a State's territorial sovereignty, the scope, scale, impact or severity of disruption caused, including the disruption of economic and societal activities, essential services, inherently governmental functions, public order or public safety must be

[129] "Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States,". op. cit. article 3.; and "Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States," op. cit., article 2.

[130] "Award of the Permanent Court of Arbitration of 4 April 1928. Island of Palmas case (Netherlands, USA)," Reports of International Arbitral Awards, accessed 14 December 2022, https://legal.un.org/riaa/cases/vol_II/829-871.pdf

[131] "Council Conclusions on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU," Council of the European Union, 20 November 2017, accessed 14 December 2022, https://www.consilium.europa.eu/media/31666/st14435en17.pdf

[132] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017), 13, https://doi.org/10.1017/9781316822524

assessed. The regime does not refer to sovereignty but determines through this list of factors when a cyber-attack is wrongful.

It is interesting to note the causal link made between "the scope, scale, impact or severity of disruption caused" and the carrying out by the state of inherently state functions such as "economic and societal activities, essential services, critical State functions, public order or public safety".[133] This causal link between the scope, scale, impact or severity of a cyber-attack and the carrying out by the state of its inherent state functions demonstrates the analogy with territorial sovereignty in cyberspace. Such approach chosen by the cyber sanctions regime is clever as it enables member states to take actions with regards cyber-attacks that cause harmful effects on EU territory.

For instance, the WannaCry ransomware attack which started in May 2017 led the EU to adopts its first sanction against persons and entities responsible for this cyber-attack. Consequently, the Council targeted the North-Koran company Chosun Expo. Indeed, it supported and facilitated this cyber-attack leading to the disruption of information systems around the world affecting EU companies and causing significant economic losses.[134] As a matter of fact, the attack hit the UK national healthcare system, which left hospitals and doctors unable to access patient data and led them to the cancellation of operations and medical appointments.[135] The severity of the WannaCry attack disrupted the UK national healthcare system, part of the essential services and critical functions the state must ensure. The WannaCry attack violated the British territorial sovereignty affecting its public health functions.

b) the number of natural or legal persons, entities or bodies affected;

The more victims the cyber-attacks make, the larger the damages and destructive consequences, thus, the more significant effect the cyber-attack has. This quantitative criterion is quite logic.

The WannaCry ransomware attack became quickly a worldwide cyberattack by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency.[136] The attacks

[133] Harriet Moynihan, "The Application of International Law to State Cyberattacks. Sovereignty and Non-intervention," Research Paper, *International Law Programme* (2019): 23
[134] "Council Decision (CFSP) 2020/1127 of 30 July 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States," op. cit., annex.
[135] Ivan, op. cit., 4.
[136] Ibid.

have affected around more than 300,000 computers across 150 countries.[137] Several companies, including EU companies, were affected by this attack, namely the carmakers Renault, Nissan and Honda which forced them to reduce or stop their production in France, the UK, Romania, Slovenia, Japan and India.[138]

Moreover, the worldwide NotPetya cyberattack of 2017 affected gravely hundreds of thousands of computers, causing damages amounting to more than USD 10 billion.[139] In Europe, TNT Express, a subsidiary of FedEx, lost around USD 400 million as a result of the attack.[140] The Danish company A.P. Moller-Maersk, the world's largest container shipping company, saw a large part of its IT infrastructure taken offline, creating a loss of USD 200-300 million.[141] The pharmaceutical company Merck & Co, one of the largest in the world, had to shut down production of one of its paediatric vaccines and lost an equivalent size of money.[142]

However, this quantitative criterion is broad and imprecise. Indeed, from what number of victims will the cyber-attack be considered to have significant effect? In that sense, the criterion is not precise enough.

c) the number of Member States concerned;

The more member states are concerned, the more the EU is affected by the cyber-attack, thus, the more significant effect the cyber-attack has. This quantitative criterion is quite logic.

EU's Member States have been victims of the disastrous and huge WannaCry and NotPetya cyber-attacks that had destructive consequences on their economy. It led to the disruption of information systems affecting EU companies, thus EU member state such as France, the UK (at the time was still member of the EU), Romania, Slovenia, Denmark.

As the former quantitative criterion, its broad sense explains its imprecision. Again, from what number of Member States concerned will the cyber-attack be considered to have significant effect? If only two member states are affected, it is sufficient to consider the cyber-attack as having significant effect? In that sense, the criterion is broad and imprecise.

---

[137] Ibid.
[138] Ibid.
[139] Ibid.
[140] "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," Andy Greenberg, Wired, accessed 10 November 2022, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
[141] Ivan, op. cit., 4.
[142] Ibid.

d) the amount of economic loss caused, such as through large-scale theft of funds, economic resources or intellectual property;

The amount of pecuniary damages the cyber-attack causes is important is assessing whether the latter has significant effect. The larger the economic loss, the bigger the damage, the more destructive the cyber-attack.

For instance, the Council targeted the North-Koran company Chosun Expo for the WannaCry ransomware attack. Indeed, it supported and facilitated this cyber-attack leading to the disruption of information systems around the world affection EU companies and causing significant economic losses.[143] The attack has affected around more than 300,000 computers across 150 countries causing a damage estimated between to USD 4 to 8 billion.[144] Moreover, the Council found Chosun Expo involved with cyber-attacks the Polish Financial Supervision Authority and Sony Pictures Entertainment, as well as cyber-theft from the Bangladesh Bank and attempted cyber-theft from the Vietnam Tien Phong Bank.[145]

Moreover, the worldwide NotPetya cyberattack affected gravely hundreds of thousands of computers, causing damages amounting to more than USD 10 billion.[146]

Furthermore, the Operation Cloud Hopper cyber-attack from 2017 attack targeted information systems of multinational companies in six continents, including companies located in the EU, and gained unauthorised access to commercially sensitive data.[147] Operation Cloud Hopper resulted in significant economic loss, notably for the EU company Swedish Ericson.[148]

e) the economic benefit gained by the perpetrator, for himself or for others;

If the cyber-attack's perpetrators gain financial benefits, then it is all the more criminalising because there is a financial motivation behind the malicious cyber act. The benefit

[143] "Council Decision (CFSP) 2020/1127 of 30 July 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States," op. cit., annex.
[144] Ivan, op. cit., 4.
[145] "Council Decision (CFSP) 2020/1127 of 30 July 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States," op. cit., annex.
[146] Ivan, op. cit., 4.
[147] "Council Decision (CFSP) 2020/1127 of 30 July 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States," op. cit., annex.
[148] Kapsokoli, op. cit., 495.

can be gained for the non-state perpetrator. However, it can also be delivered to another entity such as the foreign governments that support the cyber-attacks.

f) the amount or nature of data stolen or the scale of data breaches;

Logically, if the amount of data stolen by the perpetrator of cyber-attacks is huge, the consequences, either financial, or moral will be huge. The cyber-attack will have a significant effect.

Indeed, it can be shown with the NotPetya attack of June 2017 and the cyber-attack against the Ukrainian power grid in 2015 and 2016.[149] These attacks rendered data inaccessible in a number of EU companies by targeting computers with ransomware and blocking access to data, resulting, *inter alia*, in significant economic losses.[150]

Moreover, the 2015 cyber-attack over the Bundestag, known as the Bundestag Hack. The Bundestag Hack targeted the German Parliament's information system and affected its ability to operate for several days.[151] It resulted in the exfiltration of 16GB of data, including that of Chancellor Angela Merkel.[152] First, the amount of data in this case was huge, but it was also sensitive as it concerned information about politicians and thus of the critical State functions.

g) or the nature of commercially sensitive data accessed.

The more commercially sensitive the data is accessed, the more the security of companies is at stake. If the breach concerns sensitive data, it can result to moral damage and breach of fundamental rights to the victims. It can ruin the reputation of a company of example.

The Operation Cloud Hopper cyber-attack from 2017 attack targeted information systems of multinational companies in six continents, including companies located in the EU, and gained unauthorised access to commercially sensitive data.[153] As a result the sanctions targeted two Chinese citizens as well as the Huaying Haitai Technology Development Company for allegedly being involved in the Operation Cloud Hopper cyber-attack.

[149] "Council Decision (CFSP) 2020/1127 of 30 July 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States," op. cit., annex.
[150] Ibid.
[151] "EU sanctions two individuals and one body over 2015 Bundestag hack," op. cit.
[152] Ibid.
[153] "Council Decision (CFSP) 2020/1127 of 30 July 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States," op. cit., annex.

To sum up, the legal framework for cyber restrictive measures gives a broad, thus imprecise, list of criteria. An assessment on a case-by-case basis is necessary for each cyber-attack. Therefore, they give the Council quite some arbitrary prerogative in assessing whether a cyber-attack has significant effect, to the detriment of the principle of legal certainty. However, this arbitrary decision-making possibility given to the Council has its counterpart. Indeed, the imprecise listings criteria also give leverage to the CJEU under its judicial review which can verify, for example, whether the sanction taken by the Council is sufficiently proportional to the to the scope, scale, duration, intensity, complexity, sophistication and impact of the cyber activity.

2.2.3.4. Constituting an external threat

Furthermore, only "cyber-attacks constituting an external threat" can fall under the scope of this newly cyber sanctions regime. Here again the Council details a list of four alternative criteria, which suggest different types of links, more or less close, with the outside of the Union. Indeed, cyber-attacks constituting an external threat include those which:

1. originate or are carried out from outside the EU;

The WannaCry ransomware cyber-attack was carried out from outside the EU as the originator was North Korea. The Council targeted the North-Koran company Chosun Expo for the WannaCry ransomware attack. Indeed, it supported and facilitated this cyber-attack leading to the disruption of information systems around the world affection EU companies and causing significant economic losses.[154]

2. or use infrastructure outside the EU;

If the cyber-attack perpetrators use infrastructures that are not located within EU territory, then the cyber-attack will be considered to constitute an external threat.

3. or are carried out by persons or entities established or operating outside the EU;

For a cyber sanction to be adopted, the attacker of the cyber-attack must be located outside the EU or operate outside the EU. For instance, the Main Centre for Special

[154] "Council Decision (CFSP) 2020/1127 of 30 July 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States," op. cit., annex.

Technologies (GTsST) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU) operated the NotPetya attack from outside the EU as it is based in Russia.

4. or are carried out with the support of person or entities operating outside the EU.[155]

The external element will be met if the perpetrator of the attack operated it under the control of a foreign company or government.[156] That was the case for the major cyber-attacks WannaCry and NotPetya. They were mostly supported by foreign governments, namely North Korea and Russia in this present case.[157]

Among other things, cyber-attacks are endowed with an external element which indicates that a cyber-attack comes from the outside of EU's territory. Thus, the cyber sanctions regime applies to cyberattacks within the territory of the EU as long as there is this external element to the cyberattack.[158]

2.2.3.4.1. "a threat to the Member States"

Moreover, the regime is applicable in case of cyber-attacks constituting "a threat to the Member States" or "a threat to the Union". Thereby, a cyber-attack constituting a threat to Member States include those affecting information systems relating to (a) critical infrastructure essential to the vital functions of society, or citizens' health, safety, security, and economic or social well-being; (b) services necessary for essential social and economic activities, in particular energy, transport, banking; finance, healthcare, drinking water, digital infrastructure; (c) critical state functions, in particular defence, the governance and functioning of institutions, public elections, economic and civil infrastructure, internal security, and external relations, including diplomatic missions; (d) the storage or processing of classified information; or (e) government emergency response teams.[159] The cyber-attacks threatening Member States may

[155] "Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States,". op. cit., article 1, paragraph 2.; and "Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States," op. cit., article 1, paragraph 2.
[156] Pawlak, and Biersteker, op. cit., 35.
[157] Miadzvetskaya, and Wessel op. cit., 435.
[158] Pawlak, and Biersteker, op. cit., 35.
[159] "Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States,". op. cit., article 1, paragraph 4.; and "Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States," op. cit., article 1, paragraph 4.

trigger the imposition of cyber sanctions if they affect information systems of the above various sectors, sectors that affect the economic, social, sovereign or political function of a country.

For instance, the WannaCry ransomware attack hit the UK national healthcare system, which left hospitals and doctors unable to access patient data and led them to the cancellation of operations and medical appointments.[160] The attack affected the UK critical infrastructure essential to the citizens' health and safety and the services necessary for healthcare.

Moreover, the Bundestag Hack targeted the German Parliament's information system and affected its ability to operate for several days.[161] It resulted in the exfiltration of 16GB of data, including that of Chancellor Angela Merkel.[162] Thus the attack affected the critical state function, in particular the governance and functioning of German institutions.

Actually, the adoption of this second cyber sanctions package was more difficult than it was for the first one. Indeed, during the deliberations it was unclear whether other significant cyber-attacks against the critical infrastructure of other EU member states would be included within the sanctions package.[163] In particular, whether the 2017 Macron Leaks of supposedly internal documents of his campaign during the 2017 French presidential election.[164] In fact, this last attack was not included in the second cyber sanctions package which shows the lack of coherent resilience strategy.

2.2.3.4.2. or "a threat to the Union"

Further, the legal framework for cyber sanctions explains what a cyber-attack constituting a threat to the EU means. It corresponds to cyberattacks carried out against its institutions, bodies, offices and agencies, its delegations to third countries or to international organisations, its common security and defence policy (CSDP) operations and missions and its special representative.[165] So, whenever cyber-attacks threaten the security and foreign policy of

---

[160] Ivan, op. cit., 4.
[161] "Council Decision (CFSP) 2020/1537 of 22 October 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States," Council of the European Union, OJ L 351I, 22 October 2020, Annex, http://data.europa.eu/eli/dec/2020/1537/oj
[162] "EU sanctions two individuals and one body over 2015 Bundestag hack," op. cit.
[163] ''Europe has no strategy on cyber sanctions," Stefan Soesanto, Cybersecurity and deterrence, Lawfare Institute in Cooperation with Brookings, accessed 10 October 2022, https://www.lawfareblog.com/europe-has-no-strategy-cyber-sanctions
[164] Ibid.
[165] "Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States,". op. cit. article 1, paragraph 5.; and "Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States," op. cit., article 1, paragraph 5.

the EU or its Member States, that will constitute a threat to the EU being able to trigger the imposition of cyber sanctions.

2.2.4. Grounds for the listing and regular review

As in the general regime for restrictive measure, the targeted persons must be enlisted in the Annex of the cyber sanctions regime. Once the Council decides to impose a travel ban and/or a freezing of funds acting by unanimity, the targeted persons will be listed in the Annex of Decision CFSP 2019/797 and in the Annex I of Regulation 2019/796.[166] The Annex must include the grounds for the listing of targeted persons.[167] Indeed, in compliance with the principle of legal certainty, the Council shall communicate the sanctions, including the legal and material grounds for the listing of targeted persons, either directly or through the publication of a notice.[168] The principle of legal certainty also requires for a transparent and effective de-listing procedure. This is also to ensure the credibility and legitimacy of the restrictive measures. Thus, the legal framework provides for yearly based review for the Regulation and a regular review for Decision.[169]

These constant reviews of the listings of sanctions imposed also follows from the fact that the cyber sanctions regime shall respect the fundamental rights and the principles recognised by the Charter of Fundamental Rights of the EU, especially the right to an effective remedy and a fair trial and the right to the protection of personal data.[170] In truth, the taking into account of fundamental rights when imposing restrictive measures arose from the CJEU caselaw. In its famous *Kadi II* case, the Court demanded that listings should be accompanied by an up-to-date, defendable and clear statement of legal reasoning and the necessary material

[166] "Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States,". op. cit., article 6.; and "Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States," op. cit., article 13.
[167] "Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States," op. cit., article 14.
[168] Ibid., article 13.
[169] "Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States,". op. cit., article 10.; and "Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States," op. cit., article 13, paragraph 3.
[170] "Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States," op. cit.

information in accordance with the right for a fair trial, the right to an effective remedy, and the principle of proportionality.[171]

Thus, when adopting the first cyber sanctions, the Council adopted Decision (CFSP) 2020/1127 and Regulation (EU) 2020/1125 amending and updating the cyber sanctions regime. Thus, the names of the targeted persons and entities responsible for the abovementioned cyber-attacks have been annexed to the Decision 2019/797 and Regulation 2019/796.

Among the targeted persons, it is notable from a sovereignty perspective that the EU sanctioned four Russian nationals members of the Unit 74455 of Russia's military intelligence agency (GRU). Indeed, these four Russian agents participated in the attempted hacking into the Wi-Fi network of the OPCW in the Netherlands in April 2018.[172] Logically, the Council also targeted and enlisted the Main Centre for Special Technologies (GTsST) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU).

Also, the sanctions targeted two Chinese citizens as well as the Huaying Haitai Technology Development Company for allegedly being involved in the Operation Cloud Hopper cyber-attack. Indeed, Huaying Haitai which provided financial, technical or material support for Operation Cloud Hopper employed these two Chinese citizens.

Finally, the Council targeted the North-Koran company Chosun Expo for the WannaCry ransomware attack. Indeed, it supported and facilitated this cyber-attack.

A few months later, on 11 September 2020, discussions among the Horizontal Working Party on Cyber Issues started on whether a second package of cyber sanctions should be adopted.[173] It focused on the 2015 cyber-attack over the Bundestag, known as the Bundestag Hack. Finally, on 22 October 2020, the EU imposed cyber sanctions for the second time with Decision (CFSP) 2020/1537 and Regulation (EU) 2020/1536. Indeed, the Council adopted restrictive measures against two Russian individuals and the GRU that were responsible for or took part in the cyber-attack on the German Federal Parliament (Deutscher Bundestag) in April

[171] "Judgment of the Court (Grand Chamber) of 18 July 2013. European Commission and Others v Yassin Abdullah Kadi. Joined Cases C-584/10 P, C-593/10 P and C-595/10 P," EUR-Lex, accessed 23 November 2022, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A62010CJ0584

[172] "Council Decision (CFSP) 2020/1127 of 30 July 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States," op. cit., annex.

[173] "Europe has no strategy on cyber sanctions," op. cit.

and May 2015.[174] The Council enlisted Dmitry Badin, an officer of the GRU, and Igor Kostyukov, the head of the GRU as well as the GRU Unit 26165 (known as APT28).[175]

To summarise, the new cyber sanctions regime established by both Decision 2019/797 and Regulation 2019/796 from 17 May 2019 applies to cyber-attacks with a significant effect, including attempted cyber-attacks with a potentially significant effect, which constitute an external threat to the Union or its Member States and also to cyber-attacks with a significant effect against third States or international organisations, if deemed necessary.

The new EU cyber sanctions regime is an autonomous and decentralised sanctions regime which follows the traditional two-step procedure stemming from articles 29 TEU and 215 TFEU. The cyber sanctions regime consists of conventional restrictive measures, namely bans on persons travelling to the EU and asset freezing. The grounds for listing are similar to other restrictive measures' regimes. However, notably, the cyber sanctions regime consists of one of the few EU horizontal sanctions regime. It is a thematic regime focusing on cyber-attacks. Therefore, the legal attribution, meaning the assessment of the criteria for enlisting a person found responsible for a cyber-attack, only applies to the cyber sanctions regime. Indeed, the definition of cyber-attack is unique and has been adopted specifically for the purpose of the cyber sanctions regime. However, in order to assess the "significant effect" of a cyber-attack, the cyber sanctions regime applies the international law principle of state territorial's sovereignty applicable to cyberspace. Yet, this listing criteria are broad and unclear. Unlike other EU sanctions regime, this is a difficulty specific to the notion of cyber-attacks. Cyber-attacks are very distinct due to intrinsic features of cyberspace such as internet structural design and anonymity.[176]

Hence, the Cyber Diplomacy Toolbox, by instituting a new cyber sanctions regime, constitutes a highly symbolic diplomatic and legal contribution to the EU sanctions regime in the cyberwar context. Nonetheless, the intergovernmental character of CFSP represents a limit to the effective impact of the EU cyber sanctions regime in the context of recurring and increasing cyberattacks (part 3).

[174] "EU sanctions two individuals and one body over 2015 Bundestag hack," op. cit.
[175] "Council Decision (CFSP) 2020/1537 of 22 October 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States," op. cit., annex.
[176] Miadzvetskaya, and Wessel op. cit., 430.

3. The intergovernmental character of the CFSP, a limit against the cyberwar context

The Cyber Diplomacy Toolbox is an instrument developed by the EU under its foreign and security policy. Indeed, EU's cyber deterrence and security strategy follows the international law principle of due diligence which the Cyber Diplomacy Toolbox has enshrined (3.1.). However, the cyber sanctions regime is not is its essence an international law mechanism holding third states responsible. Thus, the principle of due diligence is undermined by Member States due to the main challenge they are facing regarding cyber-attacks; namely the policy of attribution (3.2). The attribution remains a significant challenge which is linked with the intergovernmental nature of CFSP. Notably, the collection of evidence, linked with the technical attribution, appears to be a loophole for the cyber sanctions' judicial review (3.3.).

3.1. The principle of due diligence enshrined in the Cyber Diplomacy Toolbox

The EU's cyber deterrence ambition is based on the international principle of due diligence. Due diligence is a well-accepted international law principle which finds its origin in the *Corfu Channel* case of the International Court of Justice. According to this famous case, the Court stated "every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States".[177] Thus, it follows from this definition that the principle of due diligence does not require an obligation of result but rather an obligation of conduct. The EU must ensure that rules are upheld in its own territory but also needs to assume responsibility for the repercussions of its actions beyond its borders.[178] Indeed, when it comes to cybersecurity, the EU aims at creating an open, global, free, peaceful and secure cyberspace. Hence, the principle of due diligence is enshrined within the Cyber Diplomacy Toolbox.

Indeed, it is notable to highlight the fact that the EU strongly upholds that international law applies to cyberspace and emphasises that respect for international law, in particular the UN Charter is essential to maintaining peace and stability.[179] Indirectly, the EU upholds to the

[177] "Judgment of the International Court of Justice of 4 April 1949. Corfu Channel case," ICJ Reports, 22, accessed 18 November 2022, https://www.icj-cij.org/public/files/case-related/1/001-19490409-JUD-01-00-EN.pdf
[178] Bendiek, op. cit., 69-70.
[179] "Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities," op. cit.

international principle of due diligence in cyberspace. Yet, this important role due diligence has in cybersecurity stems from the work of the UN's Group of Governmental Experts (GGE). Indeed, in its final report of June 2015, it incorporated the principle of upholding due diligence. Thus, the UNGGE affirmed that states should ensure that their sovereign territory and the computer systems and infrastructure located there, or under their control, are not used to launch attacks on the infrastructure of other states.[180] In other words, the UNGEE in this report recalls the importance of territory sovereignty which also applies to cyberspace. Two counterparts are attached to this sovereignty. The sovereign state has the right to ensure its territorial integrity is respected; yet, it also has the obligation not to use its territory so as to undermine the territorial integrity of another sovereign state.[181] Thereby, sovereign states have an obligation of due diligence on the physical or digital, national or foreign actions occurring in their territory, or under their control.[182] It must undertake everything in its power so as to ensure no cyber-attacks originating from its territory will breach another state's territorial integrity and cause significant damage. The principle of diligence is thus an obligation of conduct and not of result. A state will be held responsible for not having taken all the necessary acts to prevent and mitigate the cyber-attack from happening.

Undeniably, the principle of due diligence is at the heart of the Cyber Diplomacy Toolbox following its purpose to mitigate and prevent cyber-attacks from happening. The Cyber Diplomacy Toolbox developed CFSP instruments in order to support EU's cyber deterrence strategy. Notably, the restrictive measures are one of the Cyber Diplomacy Toolbox's instruments. Unsurprisingly, when adopting sanctions against cyber-attacks, the EU must ensure they follow and respect the CFSP goals as provided by article 21 TEU. Among those CFSP objectives, when adopting cyber restrictive measures, the EU must ensure the support to the principles of international law.[183] Subsequently, not only EU's Cyber Diplomacy Toolbox, but also cyber restrictive measures, shall consider the principle of due diligence when contributing to a safer cyberspace.

Nevertheless, when it comes to the support of the principle of due diligence by the EU through its CFSP instruments, there are some noticeable limits that cannot be ignored. It is true that the UNGGE acknowledges and considers the principle of due diligence to be a fundamental

[180] "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," United Nations Secretary General, 22 July 2015, A_70_174-EN.pdf
[181] Pawlak, and Biersteker, op. cit., 63.
[182] Ibid.
[183] "Consolidated Version of the Treaty on European Union signed on 13 December 2007," op. cit., article 21, paragraph 2, sub-paragraph b.

principle in cyberspace. This acknowledgement is also followed by a number of states, including EU Member States. Indeed, states such as Germany, Finland, France are in favour of recognising the principle of due diligence being legally binding in cyberspace.[184] However, the recognition of this principle is not without opposition from states such as the United States or Russia.[185] Thus, this lack of consensus that exist in the UNGGE materialises also within the EU. This lack of coherence between Member States with regards the recognition of due diligence as an internationally binding principle flows from the misunderstanding of the principle due diligence in itself. As being an obligation of conduct, due diligence does not engage states to be aware of all malicious cyber activities happening on their territory, nor to prevent all from happening.[186] Rather, it demands states to be reasonably diligent with regards to the cyber activities conducted on their territory. In other words, it presumes that states took all reasonable measures to prevent and mitigate the cyber-attacks occurring on their territory. Obviously, the degree of diligence stemming from states shall be of a "good Government".[187] That means that it is dependent on the legal system and structure of governance of the state so as to ensure sufficient control over the cyber activities.

Thus, this degree of diligence expected from member states is linked with the intelligence capabilities of each state. The degree of diligence expected will not be the same for states that have efficient cyber defence capabilities compared to others that do not. This is exactly the problem the EU is facing regarding cyber-attacks. As different member states do not enjoy the same cyber defence intelligence services, it results a lack of coherence and most significantly a fragmented attribution process to cyber-attackers.

Needless to say, attribution policy is a thorny issue for the EU and its Member States. Especially when it comes to the attribution of a cyber malicious act, the structure and feature of anonymity and dissimilation techniques linked to cyber-attacks renders the attribution to cyber-attacks' perpetrators extremely difficult. From a technical point of view, only a few member states are equipped with sufficient technical cyber defence capacities.[188] That is the

[184] Marc Watin-Augouard, and Guillaume Klossa, "Making cybersecurity the cornerstone of European Digital Sovereignty," 28 Recommendations for the French Presidency of the Council of the European Union on Digital Security and Regulation, *Agora FIC* (2021): 13, https://agora-fic.com/wp-content/uploads/2022/08/Agora_FIC_2021_White_Paper_Cybersecurity_Europe_EN.pdf
[185] Ibid.
[186] Pawlak, and Biersteker, op. cit., 64.
[187] International Law Commission (ILC), "Draft articles on Prevention of Transboundary Harm from Hazardous Activities*," 2001 Yearbook of the ILC,* p. 155.
[188] Pawlak, and Biersteker, op. cit., 67.

case for France, Germany, Sweden, the Netherlands, Estonia and Austria.[189] Out of twenty-seven members, only six have reliable attribution capabilities as well as the political will to share these sensitive information with other states.[190] So in terms of ensuring the respect for due diligence in cyberspace, it appears inequitable on the EU territory. Some member states are better equipped compared to others.

Furthermore, from a political point of view, reaching a collective attribution by the EU remains a challenge. Indeed, attribution of cyber-attacks is a sovereign prerogative of each member state. Hence, as few member states have sufficient cyber intelligence information, and are not necessarily willing to share them with other member states for political and strategical reasons, collective attribution is hard to reach.[191] Therefore, this fragmented attribution policy undermines the principle of due diligence in cyberspace.

The lack of coherence resulting from the attribution policy challenge represents an obstacle in ensuring fair due diligence in cyberspace between member states. Consequently, as being enshrined in the Cyber Diplomacy Toolbox, the credibility of EU's cyber diplomacy seem compromised. Due to EU's CFSP intergovernmental nature, the whole policy of attribution for cyber-attacks appears to be a deter to the credibility of EU cyber diplomacy (2.2.)

3.2. The policy of attribution, a deter to the credibility of EU cyber diplomacy

For a cyber sanction to be adopted proportionally to the behaviour of the cyber-attacker, it requires to go through the preliminary step which is attribution. For the EU to reach its goal to deter and respond to cyber-attacks, it must undergo the whole policy of attribution. Nevertheless, attribution is undeniably one of the thorniest challenge for the EU when it comes to imposing cyber sanctions. This is due to the fact that the attribution process is linked with the intergovernmental nature of the CFSP, and in particular remaining a prerogative for its member states only.[192]

[189] Bendiek, and Schulze, op. cit., 8.
[190] Ibid.
[191] Pawlak, and Biersteker, op. cit., 67.
[192] Watin-Augouard, and Klossa, op. cit., 15.

Obviously, cyber sanctions must be the result of the whole attribution process. Attribution simply refers to the process of assigning responsibility for a malicious behaviour or an act to a perpetrator.[193] So, before targeting a person or an entity, the EU needs to determine the origin of the cyberattack in a careful, and reasonable way.[194] Then, it needs to link the cyberattack to an individual or an entity. Basically, for the EU to target an individual or an entity it first needs to locate the origin of the cyber-attack leading to the potential responsible cyber-attacker. The attribution is fundamental for adopting cyber sanctions as it enables the EU to identify the perpetrators of the cyber-attacks. Thus, by identifying them, the EU can target and enlist them by adopting cyber sanctions.

The cyber sanctions regime underlines the targeted nature of restrictive measures. It is clear about the fact that the attribution of targeted persons is different from the attribution of responsibility for cyber-attacks to a third state.[195] Indeed, cyber sanctions aim at targeting persons and entities not third states and thus, categorically exclude the attribution to a third state. The attribution to a third state remains a sovereign political decision taken by EU's member states on a case-by-case basis.[196] As attribution remains a prerogative to the member states, they are free to publicly attribute cyber-attacks to a third state. Thus, the EU does not have any prerogatives for the attribution of responsibility for cyber-attacks to third countries. The EU merely plays the role of coordinator, gatherer and sharer of forensic evidence collected by the intelligence capabilities of its institutions and its member states.[197] Therefore, attribution appears to be a problem, especially a political challenge, as attribution remains a prerogative in the hands of member states which is linked with the CFSP's nature. Moreover, although cyber sanctions are aimed at targeting individuals and entities responsible for cyber-attacks only, the delimitation between targeted sanctions and attribution of responsibility of a third state is quite superficial.[198] Indeed, it appears to be politically difficult to differentiate between the nationality of location of a perpetrator of a cyber-attack and the potential state-sponsor.[199] As a matter of fact, the major cyber-attacks WannaCry and NotPetya were mostly supported by foreign

[193] Pawlak, and Biersteker, op. cit., 53.
[194] Bendiek, and Schulze, op. cit., 5.
[195] "Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States,". op. cit.
[196] Ibid.
[197] Bendiek, and Schulze, op. cit., 5.
[198] Miadzvetskaya, and Wessel op. cit., 435.
[199] Pawlak, and Biersteker, op. cit., 53.

governments, namely North Korea and Russia. Therefore, attribution is a thorny challenge that the EU must overcome in order to implement cyber sanctions.

The process of attribution is a three-levelled process which Annegret Bendiek and Matthias Schulze defines as "*the policy of attribution*".[200] The three levels are qualified as first the technical attribution (2.2.1.), second the political attribution (2.2.2.) and finally the legal attribution (2.2.3.).[201] The legal level is of course the indispensable one in order to adopt a cyber sanction. The legal level requires the technical level to gather sufficient evidence. Only the political level might be side-lined but undermines the credibility of the sanctions regime.

3.2.1. Technical attribution

Technical attribution is the first step in the attribution process. This is the first obstacle the EU has to overcome in order to adopt sanctions against persons responsible for a cyber-attack in the end. It consists of identifying the network or the computer of the cyber-attacker. Thus, cyber intelligence capabilities and IT forensics are involved in the process by evaluating the evidence gathered, usually the network logs or malware traces in the computers attacked.[202] Through the hypotheses concluded by the IT forensics, the technical attribution aims as identifying and knowing about the attacker's actions.[203]

The technical attribution can also be described as the forensic attribution which is based on forensic evidence.[204] Here the EU is confronted with the challenge to collect the necessary and sufficient intelligence information. In reality, gathering evidence of a cyber-attack is difficult because of internet's nature and structure. Actually, it is specific to the notion of cyber-attacks. As a matter of fact, the internet structural design and anonymity of cyberspace constitute barriers to the forensic technical attribution.[205] As being their intrinsic features, the cyber defence capabilities are confronted with this issue when seeking to identify the author of the cyberattacks. The anonymity constitutes the main problem as cyber-attackers use different deception techniques, such as spoofing or false flags in order to cover their tracks on cyberspace.[206] They also use crypto links or zombie routers to ensure their anonymity and blur

[200] Bendiek, and Schulze, op. cit., 10.
[201] Ibid.
[202] Ibid.
[203] Ibid.
[204] Calleri, op. cit., 7.
[205] Miadzvetskaya, op. cit., 283-284.
[206] Ibid.

their tracks in cyberspace.[207] Moreover, the location of the IP address is not sufficient and does not amount to a solid evidence as the cyber-attacker has the ability to alter or hide the location of it.[208] Intelligence capabilities collect technical evidence to support their attribution to a cyber-attacker which takes the following form such as malware computer code, IP addresses, logs, repeated patterns of activity, etc.[209] Yet, these technical evidence do not always seem strongly reliable. For instance, the location of the IP address does not amount to a solid evidence as the cyber-attacker can alter or hide the location of it.[210] Thus, the technical attribution consists of a thorny struggle for intelligence capabilities as the technical evidence can be falsified and blurred by the cyber-attackers through their deception techniques.

As the EU has no prerogatives for the attribution, it has no real operator role in the process. Therefore, it relies on the intelligence capabilities of its EU institutions and its member states. The member states play a significant part within the technical attribution phase with their intelligence services. They are the actors able to collect and gather the necessary information to identify the cyber-attacker. The problem is that not all member states are equal in this matter. Only a few member states have the sufficient technical cyber intelligence capabilities to attribute a cyberattack. This is the case for Sweden, the Netherlands, Estonia, Austria, France and Germany.[211] Necessarily the lack of sufficient intelligence capabilities for the technical attribution demonstrates its deficiency and incompleteness.

This is even more apparent when it comes to the sharing of sensitive information between member states. The previous cyber sanctions adopted by the EU have shown the lack of coordination and collaboration there is between member states. Indeed, they are usually reluctant to share sensitive information to other member states via the EU Intelligence and Situation Centre (EU INTCEN), the intelligence analysis unit of the European External Action Service (EEAS).[212] Sharing sensitive information they have gathered and collected with difficulty is not without consequence. They take the risk to compromise and expose cyber capabilities and classified cyber information with regards their public interest.[213] It would reveal the methods and techniques used by the intelligence services of the member states. The problem is that cyber-attackers could identify the weaknesses of the member states' capabilities and use

[207] Kapsokoli, op. cit., 493.
[208] Ibid.
[209] Pawlak, and Biersteker, op. cit., 61.
[210] Ibid.
[211] Bendiek, and Schulze, op. cit., 8.
[212] Ibid.
[213] Kapsokoli, op. cit., 495.

the shared information for their malicious activities to become more effective.[214] For instance this is what happened for the NotPetya attack which was more effective than the WannaCry attack. The former used the shared evidence from the latter to its benefit.[215] This explains why the member states are unwilling politically to share their evidence. This represents a significant challenge to the EU, especially as only a few members have effective intelligence capabilities. The EU here merely tries to gather the information collected from its member states and its own institutions such as Europol or EU INTCEN.

Subsequently, because of the lack of sufficient evidence collected from its member states' intelligence capabilities, the EU relies heavily on intelligence services from third countries, in particular from the Five Eyes alliance's countries.[216] Indeed, the lack of coordination between member states undermines the prompt technical attribution process which is fundamental for a cyber sanction to be adopted. Therefore, the EU relies on evidence collected by cybersecurity services of the United States and the United Kingdom mainly.[217] The practice from previous cyber sanctions adopted by the EU for the WannaCry and NotPetya cyber-attacks demonstrates this phenomenon. As a matter of fact, the EU imposed sanctions against persons and entities responsible for the WannaCry ransomware attack and the NotPetya cyber-attack in July 2020. Yet, the EU attribution was based principally on evidence and information gathered by the U.S. security services.[218] Similarly, regarding the EU sanctions adopted against the Bundestag Hack in 2015, the attribution was dependent on non-public information made between Germany and the United States.[219]

Therefore, to overcome the lack of sufficient evidence collected, the improvement of sharing of intelligence information is essential. So, a first proposal could be to strengthen the technical cyber capabilities of most EU member states. Obviously, this requires significant investments in both human and technical capabilities.[220] Regarding the former, it means that the EU should invest more in the training of cybersecurity experts and should fund EU Member States that lack mostly cyber capabilities.[221] This will ensure a more harmonious and equal cyber capability within the EU. Regarding the latter, placement of sensors and digital beacons

[214] Ibid.
[215] Ibid.
[216] Bendiek, and Schulze, op. cit., 34.
[217] Ibid.
[218] Ibid. 23
[219] Ibid. 30
[220] Ivan, op. cit., 9.
[221] Ibid.

in relevant locations on the internet would allow the member states to improve their detection capabilities.[222] This will enable the EU to improve the situational awareness in cyberspace, its ability to respond and recover from cyber-attacks and thus its capacity to attribute cyber-attacks.[223]

Of course, such investments would be very costly for the EU. Therefore, the EU should focus on developing the sharing of intelligence information. As EU member are sovereign with regards to the sharing of information, the EU should try to strengthen its capabilities from the EU INTCEN. The EU INTCEN is the "*civilian intelligence function of the EU*"[224] which gathers and analyse the information stemming from EU Member States' intelligence and security services. From that it provides an in-depth analysis of the shared situational awareness enabling the EU to further act in consequence.[225] Hence, strengthening the EU INTCEN would be a compromised solution with regards the evidence collection challenge.

Furthermore, to enhance the collection of evidence at the EU level, the EU should develop cooperation with the private sector. Indeed, to ensure a resilient and effective cyber sanctions regime, the EU shall rely on good cooperation with the private sector, as most of the cyber activities occur over infrastructures the private sector owns or operates.[226] As most of the cyber-attacks target private companies, they are frequently in a better position to provide in-depth technical analysis of these malicious cyber activities. Thus, through their computer forensic capabilities, private companies can offer valuable information to the EU.[227]

As a matter of fact, the Council stressed the importance attached to the cooperation with the private sector in the 2020 Cybersecurity Strategy.[228] Indeed, it will help the EU to assess the state of cybersecurity and effectively respond to cyber-attacks. Notably, Microsoft as a private company has significantly cooperated with the EU in this regard, having shared threat analysis data with EU institutions.[229] Further, Microsoft is at the initiative and supports the European Cyber Agora forum. The latter provides for multistakeholder guidance and

---

[222] Ibid.
[223] Ibid.
[224] "EU INTCEN Intelligence Analysis Centre," EU INTCEN, *Fact Sheet*, 5 February 2015, accessed 21 November 2022, https://www.statewatch.org/media/documents/news/2016/may/eu-intcen-factsheet.pdf
[225] Ibid.
[226] Pawlak, and Biersteker, op. cit., 70.
[227] Ibid.
[228] "Draft Council conclusions on the EU's Cybersecurity Strategy for the Digital Decade," Council of the European Union, OJ 6722/21, 9 mars 2021, https://data.consilium.europa.eu/doc/document/ST-6722-2021-INIT/en/pdf
[229] Miadzvetskaya, and Wessel op. cit., 437.

cooperation on EU cybersecurity policy issues through structured exchanges between EU institutions, EU Member States, the private sector, academia, and civil society, with the aim of strengthening the collective EU vision of cyberspace globally.[230] Through this forum, Microsoft represents an important private stakeholder helping the EU to advance on global cybersecurity policy debates.

Subsequently, by sharing strategic and sensitive information the private sector becomes "*quasi-intelligence agencies*"[231]. Nevertheless, increasing the role of private companies with regards to sensitive cybersecurity information may be seen as a threat to the public interest of member states. Some member states are very concerned with regards their sovereignty for safeguarding their national security. According to article 4 TEU, the EU must ensure their essential State functions including safeguarding national security which remains the sole responsibility of each Member States.[232] So, strengthening relations with cybersecurity private companies might be considered as touching upon national sovereignty. This may lead to difficult acceptance by some public bodies and EU member states. Thus, the EU should not neglect developing its relations with the public sector as well.

Notably, the EU must enhance cooperation with international organisations such as NATO. Indeed, NATO do not have the same tools to deter cyber-attacks as the EU has, so these two organisations can be beneficial to one other as being complementary.[233] Thus, it is up to them to coordinate their responses to cyber-attacks. Last but not least, the EU upholds that international law applies to cyberspace and emphasises that respect for international law, in particular the UN Charter is essential to maintaining peace and stability.[234] So, it is logical that the EU shall continue to develop dialogues with the UN regarding cybersecurity norms so as to reach to a common purpose, i.e., deterring cyber-attacks and enhancing international cybersecurity.

Consequently, the technical attribution based on forensic evidence demonstrates an important problem for the EU cyber diplomacy and especially for its cyber sanctions regime. Obviously, such a fragmented technical attribution deters the credibility and effectiveness of

---

[230] ''Harnessing the Power of Trust,'' European Cyber Agora, *ECA Brussels Communiqué 2022*, 2022, accessed 21 November 2022, https://www.microsoft.com/en-eu/cyber-agora/
[231] Pawlak, and Biersteker, op. cit., 74.
[232] "Consolidated Version of the Treaty on European Union signed on 13 December 2007," op. cit., article 4, paragraph 2.
[233] Ivan, op. cit., 11.
[234] "Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities," op. cit.

the cyber sanctions regime. This is even more deterred by the political attribution which is linked with the intergovernmental nature of CFSP.

3.2.2. Political attribution

After having identified the origin of the cyberattack, the political attribution comes after. It is the is the phase consisting of assigning responsibility for a malicious cyber activity to a specific person or entity. It aims at linking the operation with the perpetrator of the attack, with the hope of mitigating his behaviour and refrain him from future cyber-attacks.[235] In other words, political attribution is the "naming and shaming" of the attacker.[236] In order to name the perpetrator of the attack, the states must exchange the information gathered between themselves and with the EU. This represents the main challenge for the EU because Member States are sovereign in this regard. Political attribution remains a sovereign decision which is dependent on the member states' political and national interests.[237]

A collective attribution by EU member states requires to reach unanimity within the Council.[238] Indeed, for the EU to enlist specific persons that have been found responsible for the cyber-attacks, the Council needs to take a decision at unanimity. Therefore, political attribution corresponds to an enormous challenge which stems from the CFSP decision-making procedure. Indeed, EU's CFSP is characterised by intergovernmentalism. Especially the decision-making procedure is different from that prevailing in the ordinary legislative procedure. Normally, the qualified-majority is sufficient; yet, under EU's CFSP, the legal acts must be adopted at unanimity. That means that each member state has a right to veto and are thus sovereign in this area.

Hence, collective attribution is a challenge for the EU as some member states want to retain their decision-making autonomy and thus their sovereignty.[239] Moreover, the diverse economic and political interests of each member states may form an obstacle in reaching unanimity among the Council. It is worth reminding that Italy at first firmly opposed to the idea and introduction of a new cyber sanctions regime.[240] Therefore, EU's CFSP decision-making process requiring all EU member states' governments to reach unanimity is a hurdle when it comes to political attribution. Indeed, as being politically sensitive, it might be hard for some

[235] Bendiek, and Schulze, op. cit., 10.
[236] Ibid.
[237] Calleri, op. cit., 7.
[238] Ibid.
[239] Watin-Augouard, and Klossa, op. cit., 15.
[240] "Italy resisting EU push to impose sanctions over cyberattacks", op. cit.

member states to accept to collectively attribute a person linked with a third country to which these member states have strong links with.[241]

The practice has shown the difficulty stemming from this collective attribution. Indeed, regarding the WannaCry and NotPetya attacks that happened in 2017, it took the EU three years to finally adopt sanctions against perpetrators for these attacks and thus for the Council to attain this unanimity requirement. This three-year gap time is not insignificant. While the Council condemned these attacks in its conclusions in 2018, only a few member states publicly attributed these attacks to the Russian Government this same year; notably Denmark, Latvia, Sweden and Finland.[242] It took the EU two more years to reach the unanimity requirement for a collective attribution of these attacks to Russian and North-Korean persons and entities.

Moreover, regarding the Bundestag Hack, only six out of twenty-seven member states publicly endorsed the attribution.[243] In this case, Austria, Belgium, Denmark, the Netherlands, Estonia and Latvia were the only states that nationally attributed the Bundestag Hack through government statements [244] Surprisingly, not even Germany, which encouraged the EU to adopt sanctions against this cyber-attack, publicly endorsed the second cyber sanctions package.[245] Five years after the cyber-attack occurred, the EU member states collectively attributed the Bundestag Hack to the GRU Unit 26165 (known as APT28). However, for geopolitical interests, the member states are sovereign regarding their own public attribution for a specific cyber-attack.

As a matter of consequence, this lack of coherence between member states with regard political attribution diminishes the credibility of EU's cyber diplomacy. Indeed, the lack of political communication and coherence is probably due to the inability for member states to reach unanimity and thus to act unified.[246] Therefore, political attribution is linked with the member states' political willingness and interests. Obviously, reaching unanimity, as part of the CFSP intergovernmental nature, is a challenge for the EU. So, it undermines the credibility of the Cyber Diplomacy Toolbox and consequently the cyber sanctions regime.

[241] Ivan, op. cit., 7.
[242] Bendiek, and Schulze, op. cit., 25.
[243] "Europe has no strategy on cyber sanctions," op. cit.
[244] Ibid.
[245] Ibid.
[246] Ibid.

3.2.3. Legal attribution

Finally, the legal attribution consists of describing the assignment of criminal blame or indictment.[247] The EU must be able to classify the attack in order to determine whether it is ranged as a cybercrime or a cyberattack. They will not fall under the same legal acts. Indeed, if a cyber malicious act is defined as a cybercrime, it will fall under the Cybercrime Directive 2013 on attacks against information systems.[248] While, if the cyber malicious act is defined as a cyber-attack, it will fall under the cyber sanctions regime. It could happen that a same cyber malicious act could be classified differently, depending on the forensic capabilities, either as a cybercrime or a cyber-attack.[249] Depending on the classification, the legal standards will not be the same.

The legal attribution is necessary and indispensable to adopt a cyber sanction. The legal attribution requires the EU to legally classify the cyber-attacks. That means to assess whether the malicious acts correspond to a cyber-attack as defined by the cyber sanctions regime under article 1 and 2 of the Regulation 2019/797. [250] Without meeting the criteria stemming from the cyber sanctions regime, the sanction cannot be adopted. Thus, for the EU to legally attribute a cyber-attack it still needs to demonstrate that it is a cyber-attack with a significant effect, which constitute an external threat to the Union or its Member States, in compliance with article 1 of the Regulation 2019/797.[251] Therefore, it is extremely important for the member states to develop a common definition of a serious cyber-attack having significant effect.[252] However, as previously analysed, the listing criteria of cyber-attacks having significant effect are unclear. Therefore, one may wonder about the reliability of technical attribution where IP addresses cannot be sufficient evidence. Yet technical evidence constitutes the basis of legal attribution according to which the EU adopts cyber sanctions.[253] Hence, legal attribution also seems to be unpredictable which at the end deters the credibility of the cyber sanctions regime.

[247] Bendiek, and Schulze, op. cit., 11.
[248] "Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA," European Parliament and Council of the European Union, OJ L 218, 14 August 2013, http://data.europa.eu/eli/dir/2013/40/oj
[249] Bendiek, and Schulze, op. cit., 11.
[250] Ibid.
[251] "Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States," op. cit.
[252] Ibid.
[253] Bendiek, and Schulze, op. cit., 35.

To conclude, both technical, political and legal attribution, namely the policy of attribution, is a thorny challenge for the EU. Indeed, the attribution policy requires to reveal the computer of network systems responsible for the cyber-attack and then to identify the perpetrator of this cyber-attack to name it. Thus, the policy of attribution is a preliminary step for the adoption of restrictive measures against cyber-attacks. Nevertheless, the main difficulties the EU is confronted with are the technical and the political attributions. With regards the former, the fragmented attribution capabilities and intelligence services between member states renders this effectiveness of the policy of attribution arduous. Moreover, the lack of collaboration between member states in sharing their sensitive information deters the effectiveness of the cyber sanctions regime since insufficient evidence is collected by the EU to adopt a sanction. With regards the latter, the unanimity requirement stemming for the CFSP's intergovernmental nature represents an important obstacle to the collective attribution. Subsequently, the EU's attribution policy demonstrates a lack of coherence between its member states. Thus, to the detriment of the credibility of EU's Cyber Diplomacy Toolbox and cyber sanctions regime.

The challenge with regards the technical attribution might also be problematic before the CJEU. Indeed, the collection of evidence appears to be a loophole for the cyber sanctions' judicial review (3.3.).

3.3. The collection of evidence: a loophole for the cyber sanctions' judicial review

As the EU legal order is based on the rule of law, the cyber sanctions can be subject to judicial review by the CJEU which ensures, through its high standard, that the fundamental rights are respected (3.3.1.). However, for a sanction to be adopted, the decision targeting the persons responsible for the cyber-attack must disclose the reasons for listings alongside with substantial evidence (3.3.2.).

3.3.1. The high standard of fundamental rights protection in the CJEU's judicial review

The cyber sanctions are not immune from the CJEU's judicial review provided under article 275(2) TFEU. First and accordingly, the cyber sanctions adopted by the Council must

include reasons for listings and substantiated with forensic evidence.[254] Second, the evidence must be disclosed to the targeted person to ensure its fundamental rights as enshrined in article 6(1) TEU are respected.[255] At the end, it is the CJEU which has the final word regarding what constitutes a sufficiently evidence based restrictive measure.

According to article 275 TFEU, although the CJEU has no jurisdiction over CFSP acts, it still has jurisdiction to review the legality of restrictive measures.[256] The CJEU can review restrictive measures through the action for annulment provided by article 263 TFEU. Article 263 TFEU provides for the action for annulment enabling the CJEU to review the legality of EU acts brought by individuals that are act addressed to them or which is of direct and individual concern to them, or against a regulatory act which is of direct concern to them and does not entail implementing measures.[257] With regards to article 275 TFEU, it seems to be the only acceptable legal remedy which shows the limits of the scope of judicial review over restrictive measures. Especially since the conditions of admissibility (personally, individually, directly affected) for the action for annulment are quite restrictive. However, in that regard, through its praetorian power, the CJUE made a broad interpretation of its jurisdiction over restrictive measures. Indeed, in its *Rosneft Oil Company* from 2017, the CJUE held it has jurisdiction to give preliminary rulings, under Article 267 TFEU, on the validity of an act adopted on the basis of provisions relating to the CFSP provided that the request for a preliminary ruling relates to reviewing the legality of restrictive measures against natural or legal persons.[258] Hence, the CJEU has jurisdiction to review the legality of restrictive measures against persons or entities responsible for cyber-attacks through either the action for annulment or the preliminary rulings.

Nevertheless, the judicial standard set by the CJEU with regards to restrictive measures is quite high. Indeed, the CJEU imposes a high fundamental rights scrutiny especially regarding due process and evidentiary standards. This stems from the well-known *Kadi* cases on anti-terrorist sanctions. In the *Kadi I* case, the CJ held that it falls within its jurisdiction to ensure in principle the full review of the lawfulness of all EU acts in the light of the fundamental rights,

[254] Miadzvetskaya, and Wessel op. cit., 436.
[255] Ibid.
[256] "Consolidated Version of the Treaty on The Functioning of the European Union signed on 13 December 2007," op. cit., article 275, paragraph 2.
[257] Ibid. article 263, paragraph 4.
[258] "Judgment of the Court (Grand Chamber) of 28 March 2017. PJSC Rosneft Oil Company, formerly OJSC Rosneft Oil Company v Her Majesty's Treasury, Secretary of State for Business, Innovation and Skills, The Financial Conduct Authority. Case C-72/15," paragraph 81, EUR-Lex, accessed 23 November 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62015CA0072

including review of EU restrictive measures.[259] As the EU legal order is based on fundamental rights as enshrined in the Charter of Fundamental Rights of the European Union and the rule of law, it is for the CJEU to review any restrictive measure in respect to fundamental rights. In the *Kadi II* case, the CJEU further explained its standard of judicial review with regards to restrictive measures. In particular, the CJEU held that the listings need to be taken on a sufficiently solid factual basis, which entails a verification of the factual allegations whereby at least one of the reasons provided should support the listing.[260] Moreover, the information or evidence produced should support the reasons relied on against the person concerned.[261] Finally, it is for the Court to determine whether the reasons relied on by that authority as grounds to preclude that disclosure were founded.[262] The CJEU reviewed the contested restrictive measure with regards to the right for a fair trial, the right to an effective remedy, and the principle of proportionality.

Hence, it follows from the *Kadi II* case that the standard of review for restrictive measures is as follows. The decision enlisting the targeted persons needs to be sufficiently substantiated by evidence. Therefore, to ensure the targeted persons' right to a fair trial and to an effective remedy are respected, the listings shall be accompanied by clear, defendable statement of reasoning of the decision.[263] It also implies that the statement of reasons identifies not only the legal basis of that measure but also the individual, specific and concrete reasons behind the targeted restrictive measures.[264]

Thus, for the EU to adopt cyber sanctions, the decision targeting the persons responsible for the cyber-attack must disclose the reasons for listings alongside with substantial evidence (4.2.).

3.3.2. Disclose confidential information or evidence

As mentioned in the first part, the cyber sanctions regime relies on forensic evidence.[265] So as to forensically attribute a cyber-attack to a specific person or entity, the EU needs to rely

[259] "Judgment of the Court (Grand Chamber) of 3 September 2008. Yassin Abdullah Kadi and Al Barakaat International Foundation v Council of the European Union and Commission of the European Communities. Joined cases C-402/05 P and C-415/05 P," paragraph 326, EUR-Lex, accessed 23 November 2022, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A62005CJ0402
[260] "Judgment of the Court (Grand Chamber) of 18 July 2013. European Commission and Others v Yassin Abdullah Kadi. Joined Cases C-584/10 P, C-593/10 P and C-595/10 P," op. cit., paragraph 119.
[261] Ibid., paragraph 122
[262] Ibid., paragraph 126
[263] Ibid., paragraph 100
[264] Ibid., paragraph 116
[265] Calleri, op. cit., 7.

on evidence gathered by intelligence capabilities. As described above, it requires technical attribution – i.e., to locate the computer or the network systems responsible for the cyber-attacks and then link it to the individuals that were behind all of it. In other words, for the sanction to be established, it needs to be based on forensic evidence intelligence tracking back the perpetrators of the cyber-attacks. As Yuliya Miadzvetskaya clearly states "*no evidence should mean no sanction*"[266]. Therefore, the Council must provide for solid evidence to support its sanction listings.

However, when it comes to collecting the necessary and sufficient forensic evidence to support its sanctions' listings, the EU is confronted with several challenges. First, the listings criteria provided by cyber sanctions regime in relation to the scope of cyber malicious activities are unclear. According to article 1 Decision 2019/797, sanctions will be adopted in response to cyber-attacks with a significant effect which constitute an external threat to the EU or its Member States.[267] Indeed, the notion of "significant effect" is broadly defined by the Council with a list of factors. The notion of "significant effect" is assessed in the light of a series of blurry criteria, such as its "scope, scale, impact or severity of disruption caused" or "the number of natural or legal persons, entities or bodies affected".[268] This imprecision of listing criteria offers the Council arbitrary prerogatives in assessing whether a cyber-attack has significant effect.[269] The rationale behind this is that the broader the listing criteria are, the easier it will be for the Council to comply with the standard set by the CJEU regarding evidence and reasons requirements for sanctions.[270] Nonetheless, this ease of compliance with the CJEU's standard is far from being simple. The CJEU fundamental rights' standard regarding sanctions is quite high. It will need to strike a balance between the flexibility of the cyber sanctions regime and the legal certainty principle.[271]

A second challenge the EU is confronted with is the actual collection of sufficient and effective forensic evidence. The evidence collection of a cyber-attack is difficult as inherent to the cyberspace and internet's nature and structure. Indeed, the internet's structural design and anonymity of cyberspace constitutes barriers to the forensic evidence collection.[272] Thus, the

[266] Miadzvetskaya, op. cit., 291.
[267] "Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States,". op. cit., article 1, paragraph 1.
[268] Ibid., article 3.
[269] Yuliya Miadzvetskaya, "Cyber sanctions: towards a European Union cyber intelligence service?" *College of Europe Policy Brief* 1, 21 (2021): 3, http://aei.pitt.edu/id/eprint/103385
[270] Ibid.
[271] Ibid.
[272] Miadzvetskaya, op. cit., 283-284.

collection of technical evidence on the cyber-attackers consists of a thorny struggle for intelligence capabilities. The technical evidence can be falsified and blurred by the cyber-attackers through their deception techniques.

Furthermore, the EU also has to tackle the member states' reluctance to share collected evidence by their national intelligence services. The EU merely plays the role of coordinator of forensic evidence collected by the intelligence capabilities of its institutions and its member states. Moreover, the collection of forensic evidence regarding cyber-attacks is not facilitated by the fact that the computers or individuals involved might be located in a foreign country.[273] Hence, the identification of the persons or entities responsible for the cyber-attacks may depend on the cooperation of foreign state which could consists of an obstacle to the evidence collection for the EU. In this regards, the Budapest Convention on Cyber Crime provides for international cooperation when it comes to evidence collection for cybercrimes.[274]

Consequently, sanctions must be supported by sufficient strong and solid evidence collected by the intelligence capabilities. Indeed, when the Council adopts a cyber sanction, the annex must include the justifications and grounds for listing the targeted persons.[275] The sanctions need to provide with sufficient reasons for enlisting a specific person. In compliance with the principle of legal certainty, the Council shall communicate the sanctions, including the legal and material grounds for the listing of targeted persons, either directly or through the publication of a notice.[276] Thus, the grounds supporting the listing for targeted persons shall be based on solid forensic evidence in order to withstand the potential judicial review of the CJEU. As a matter of fact, it is up to the CJEU to decide whether the evidence on which the sanction listings is based on is sufficiently substantial.

However, revealing evidence collected by cyber intelligence services could be dangerous and could touch upon the security of the EU or of its Member States. Not all confidential information needs to be disclosed to the targeted person. Therefore, the CJEU will weigh the requirements linked to the right to a fair trial, protected by article 47 of the Charter of Fundamental Rights, with the requirements stemming from the security of the EU or of its

[273] Ibid.
[274] "Budapest Convention on Cybercrime of the Council of Europe," ETS 185, 23 November 2001, article 23, https://rm.coe.int/1680081561
[275] "Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States," op. cit., article 14.
[276] "Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States," op. cit., article 13.

Member States.[277] If the CJEU considers that the reasons for targeting persons are sufficiently substantiated, then it will strike a balance between the confidential information and the right to a fair hearing with regards to the principle of proportionality. Namely, the restrictive measures must be genuinely necessary to achieve an objective of general interest recognised by the EU and must comply with the principle of proportionality. Thus, to strike the balance, the CJEU will assess whether and to what extent the failure to disclose confidential information or evidence to the person concerned and his consequential inability to submit his observations on them are such as to affect the probative value of the confidential evidence.[278]

Consequently, in 2015 the Rules of Procedure of the General Court has been amended in order to implement the new ruling of *Kadi II* case. Indeed, article 105 states that the CJEU shall weigh the requirements linked to the right to effective judicial protection, particularly observance of the adversarial principle, against the requirements flowing from the security of the Union or of one or more of its Member States or the conduct of their international relations.[279] Yet, at the end the Court can decide to take into account information the targeted person has not had access to, if this "is essential in order for it to rule in the case and confining itself to what is strictly necessary"[280].

Subsequently, the judicial standard set by the CJEU with regards the review of cyber restrictive measures is high. Indeed, when adopting a cyber sanction, the listing of targeted persons and entities must respect fundamental rights, in particular the right to an effective remedy and to a fair trial. Since the freeze of assets could lead to the violation of the right to property and the ban of travelling to the right to freedom of movement. Thus, the sanction could lead to significant damages if incorrectly based. Evidently, the CJEU imposes a high judicial standard based on fundamental rights over restrictive measures.

As a matter of fact, the Council has lost many cases of sanctions because insufficiently evidenced.[281] Obviously, by analogy the CJEU will hold the same level of scrutiny with regards to cyber sanctions. The requirement to sufficiently substantiate by evidence the reasons for targeting persons is even harder to reach with the anonymity character inherent to cyber-attacks.

---

[277] "Judgment of the Court (Grand Chamber) of 18 July 2013. European Commission and Others v Yassin Abdullah Kadi. Joined Cases C-584/10 P, C-593/10 P and C-595/10 P," op. cit., paragraph 128.
[278] Ibid., paragraph 129.
[279] "Rules of procedure of the General Court," OJ L 105, 23 April 2015, article 105, paragraph 5, http://data.europa.eu/eli/proc_rules/2015/423/oj
[280] Ibid., article 105, paragraph 8
[281] Miadzvetskaya, "Cyber sanctions: towards a European Union cyber intelligence service?", op. cit. 1.

Hence, the Council has and will lose many cases of cyber sanctions before the CJEU's judicial review, undermining the effective impact of the cyber sanctions regime.

As the EU legal order is based on the rule of law, it is necessary for the CJEU to strike a balance between the cyber diplomacy objectives and the need to protect targeted individuals from arbitrary sanctions.[282] However, the Council's reasons for enlisting targeted persons rely mostly on intelligence information collected by Member States' intelligence services. The latter are usually reluctant to share these information which lead to insufficiently substantiated evidenced decisions. Thus, the CJEU will reject these insufficient proved cyber sanctions through its judicial review. Consequently, it undermines the effectiveness of the cyber sanctions regime.

As the CFSP is an area where member states retain their sovereign prerogatives, it is understandable that the policy of attribution cannot be effective as solely dependent on the intergovernmental character and decision-making of this policy. Therefore, a question regarding the border between the CFSP and the AFSJ in cyber-attacks might be interesting as to potentially give an answer to overcome the intergovernmental obstacles (part 4).

[282] Ibid., 2

4. The delimitation between the CFSP and the AFSJ in cyber sanctions

Evidently, security is an objective that both the CFSP and the Area of Freedom, Security and Justice (AFSJ) aim at ensuring. Hence, cybersecurity can be covered both by the CFSP and the AFSJ. Whether cybersecurity falls under the CFSP or the AFSJ will have consequences on the decision-making procedure to adopt them. For this reason, it is important first to address the decision-making procedures of both the CFSP and AFSJ (3.1.), then to raise the border clash between the CFSP and the AFSJ to better understand the cyber sanctions regime (3.2.).

4.1. Decision-making procedures of the CFSP and the AFSJ

Security is a fundamental concern for the EU and lies among the objectives of the EU as part of both its CFSP and its AFSJ.[283] Traditionally, the EU divided the internal security issues falling under AFSJ and the external security issues falling under the CFSP.[284] This divide stems from the three-pillar division established by the Maastricht treaty in 1993.

As a matter of fact, at the time emerged the idea of adding competences for the Community in fields of foreign and security matters as well as on asylum and immigration policy, criminal co-operation, and judicial co-operation. However, some Member States were reluctant in transferring a part of their sovereignty to such sensitive areas of foreign policy or justice. Thus, the idea of the three-pillar system was created in order to cope with the loss of national sovereignty in these areas. The European Community would represent the first pillar, while the second pillar would deal with foreign policy, defence and security issues, and the third pillar would allow cooperation in the judicial field.

Consequently, the CFSP was designed as an intergovernmental pillar with the aim of preserving peace, strengthening international security, promoting international cooperation and developing and consolidating democracy, the rule of law and respect for human rights and fundamental freedoms.[285] Clearly, the fact that the CFSP is intergovernmental by its nature has several consequences.[286] First, regarding the decision-making procedure, it is different from the

[283] Miadzvetskaya, and Wessel op. cit., 414.
[284] Ibid.
[285] "Consolidated Version of the Treaty on European Union signed on 13 December 2007," op. cit., article 21.
[286] "Foreign policy: aims, instruments and achievements," European Parliament, *Fact Sheets on the European Union*, 2022, accessed 17 November 2022, https://www.europarl.europa.eu/factsheets/en/sheet/158/foreign-policy-aims-instruments-and-achievements

ordinary legislative procedure subject to qualified majority. In the CFSP, as all Member States have kept their national sovereignty, all decisions have to be adopted at unanimity. That means that each member state has a veto on every decision which makes it difficult to achieve a common position. Second, several EU institutions are side-lined from the policy having limited power. The Lisbon Treaty, by abolishing the pillar system, brought some changes regarding the structure of the CFSP. It created the High Representative of the Union for Foreign Affairs and Security Policy, being a member of both the Commission and the Council, to conduct the CFSP.[287] Still, it remains a specific policy of the EU governed by its intergovernmentalism features. The European Parliament is almost side-lined with merely a consulting power. The CJEU has no jurisdiction over CFSP decisions, except to review the legality of decisions for restrictive measures.[288]

The second additional pillar established by the Maastricht Treaty was the Justice and Home Affairs (JHA). It dealt with policies such as asylum, immigration, cooperation in the judicial, customs and police fields. In 1999, the Treaty of Amsterdam introduced the idea of an area of freedom, security and justice. This treaty defined the goal of this area which the Treaty of Lisbon later completed. The Union shall offer and maintain "area of freedom, security and justice without internal frontiers, in which the free movement of persons is ensured in conjunction with appropriate measures with respect to external border controls, asylum, immigration and the prevention and combating of crime."[289] Indeed, the Treaty of Lisbon has had a significant impact on the AFSJ. As the three-pillar system has been eliminated, based on intergovernmental cooperation, it generalised the "Community method" or the "European method" – despite distinct rules govern CFSP.[290] Thus, under the AFSJ, legislative proposals are adopted under the ordinary legislative procedure set out in article 294 TFEU.[291] The European Commission has the initiative in the legislative process, the European Parliament, as co-legislator, delivers its opinions on the process and the Council, having the last word in the shuttle, acts by qualified-majority.[292] The CJEU's prerogatives have also increased with the

---

[287] Ibid.
[288] "Consolidated Version of the Treaty on The Functioning of the European Union signed on 13 December 2007," op. cit., article 275.
[289] "Consolidated Version of the Treaty on European Union signed on 13 December 2007," op. cit., article 3, paragraph 2.
[290] "An area of freedom, security and justice: general aspects,'' European Parliament, *Fact Sheets on the European Union*, 2022, accessed 17 November 2022, https://www.europarl.europa.eu/factsheets/en/sheet/150/an-area-of-freedom-security-and-justice-general-aspects
[291] Ibid.
[292] "Consolidated Version of the Treaty on The Functioning of the European Union signed on 13 December 2007," op. cit., article 294.

Lisbon Treaty in the AFSJ. Before Lisbon, the CJEU did not have full judicial review over human rights question in this field. Nor was the preliminary ruling in this field obligatory, as was dependent on Member States acceptation.[293] The Lisbon Treaty, through its generalisation of the "Community method", allows the CJEU to give preliminary rulings, without restriction, and legality review on all aspects of the AFSJ.[294]

As the CFSP is an area where member states retain their sovereign prerogatives, the border clash between the CFSP and the AFSJ in cyber-attacks might be interesting as to potentially give an answer to overcome the intergovernmental obstacles (3.2.).

4.2. The border clash between the CFSP and AFSJ in cyber-attacks: a solution to overcome the intergovernmental obstacles?

As mentioned above, the cyber sanctions regime was adopted according to the two-step approach required by EU Treaties to adopt restrictive measures under CFSP. First on the basis of a Council Decision adopted under article 29 TEU, then a Council Regulation adopted under article 215 TFEU. Accordingly, a decision adopted in accordance with the CFSP decision-making process under the TEU (i.e., unanimity) is the first step. Then, it is implemented according to the TFEU procedure (i.e., qualified-majority). Nonetheless, when it comes to the AFSJ, as regards preventing and combating terrorism and related activities, sanctions are adopted on the basis of articles 75 and 76 TFEU. They provide for different procedures involving the ordinary joint legislative power between the European Parliament and the Council. Thus, adopting sanctions under AFSJ overcomes the unanimity problem the CFSP poses and allows, through the European Parliament's involvement for democratic scrutiny. Therefore, it is interesting to raise the border clash between CFSP and AFSJ regarding cyber sanctions.

In truth, the EU's first cybersecurity initiatives were covered on the basis of the internal market clause, article 114 TFEU.[295] This article provides the EU the ability to adopt measures for the approximation of Member States' law, regulation or administrative action to ensure the establishment and functioning of the internal market.[296] At first, as the EU had no explicit legal

[293] Paul Craig, and Gráinne De Búrca, *EU Law. Text, Cases, and Material* (Oxford: Oxford University Press, 2015), 976.
[294] "An area of freedom, security and justice: general aspects,'' op. cit.
[295] Miadzvetskaya, and Wessel op. cit., 418.
[296] "Consolidated Version of the Treaty on The Functioning of the European Union signed on 13 December 2007," op. cit., article 114, paragraph 1.

basis to adopt cybersecurity legislation, it used the internal market to create an EU digital market.[297] The EU, through this broad clause, tries to expand its competence in the field of cybersecurity. This is another demonstration of the pre-emption effect in cybersecurity. The more the EU exercises a shared competence, the more it adopts a legislation, the less room there is left for the Member States within the shared competence. Shared competences tend to become exclusive as they are exercised by the EU. So, when using article 114 TFEU to legislate in cybersecurity, the EU tends to use its pre-empting power. This resulted in the NIS Directive, a significant legislation in the field of cybersecurity, which finds its legal basis on the internal market.[298] Indeed, it aims at achieving a high common level of security of network and information systems to ensure the functioning of the internal market.[299]

However, progressively the internal market was not sufficient to cope with cybersecurity issues. Indeed, the practice and increase of cybercrimes led the EU to develop cybersecurity legislation as part of the AFSJ. Notably, the Cybercrime Directive from 2013 was a major one.[300] The Cybercrime Directive, adopted on the basis of article 83(1) TFEU, aims to fight cybercrimes and contributes to the judicial cooperation in criminal matters.[301] Article 11 of the Directive provides for sanctions in response to attacks against information systems, including access to systems, systems interferences, data interference.[302] The legal person found responsible for the cybercrime can be subject to financial and non-financial sanctions such as the exclusion from entitlement to public benefits, the temporary or permanent disqualification from the practice of commercial activities, the placing under judicial supervision, the judicial winding-up or the temporary or permanent closure of establishments which have been used for committing the offence.[303] The Cybercrime Directive confirms the first steps in the EU's considerations of the external dimension of cybersecurity. This means that the EU's initiative in cybersecurity has been institutionalised vis-à-vis cyber malicious acts committed outside the EU territory. As cyber threats usually come from the outside of the EU, it is logical that the EU

[297] Miadzvetskaya, and Wessel op. cit., 418.
[298] Ibid.
[299] "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union," op. cit.
[300] "Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA," op. cit.
[301] Ibid.
[302] Ibid.
[303] Ibid., article 11.

established its cybersecurity policies into its AFSJ, but also its CFSP.[304] Thus, the EU has adopted the cyber sanctions regime in 2019 for cyber-attacks constituting an external threat.

Adopted on the basis of article 215 TFEU, the cyber sanctions regime covers malicious cyber acts that may be perpetrated by EU citizens or residents, and for which the link to international dimension sometimes appears to be weak.[305] For instance, an EU citizen organises a cyber-attack having significant effect on the EU who got the support of a person or entity acting outside of the EU. According to article 1 of Decision 2019/797, a cyber-attack which was or are carried out with the support of person or entities operating outside the EU is enough to constitute an external threat. Consequently, the external element will be met. The mere fact that there was support from outside the EU territory would demonstrate the international dimension of the threat which should fall under the scope of CFSP. However, from that perspective, the external element of the cyber-attack can be considered weak which could raise questions about the scope of Article 215 TFEU. Where the external element is limited to the fact that the perpetrator was supported by a person acting outside the EU, is this sufficient to disqualify the AFSJ? In other words, it could renew the problem of the border between CFSP and AFSJ in terms of sanctions. Whether cyber-attack constituting an external threat to the EU shall be covered by CFSP or AFSJ. It will have consequences on the decision-making procedure to adopt them.

Delimitation between the CFSP and the AFSJ regarding cyber sanctions is an important aspect in understanding the cyber sanctions regime. This is a challenge the CJEU has already been confronted with in the past regarding international agreements and anti-terrorist sanctions.

In the famous *EU-Mauritius Agreement* case, the delimitation between the CFSP and the AFSJ was at the centre of the CJEU's review. In this case the European Parliament challenged the Council's CFSP decision on the signing and conclusion of an agreement with Mauritius concerning the treatment of suspected pirates and associated seized property.[306] The agreement covered both CFSP and AFSJ issues. Therefore, the central question the CJEU was confronted with was whether the international agreement related exclusively to CFSP. If not, the agreement would fall under the ordinary legislative procedure and the Parliament would be

[304] Miadzvetskaya, and Wessel op. cit., 425.
[305] Chauvel, and Hamonis, op. cit., 746.
[306] "Judgment of the Court (Grand Chamber) of 24 June 2014. European Parliament v Council of the European Union. Case C-658/11," EUR-Lex, accessed 16 December 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62011CJ0658

consulted and could give its consent according to article 218(6) TFEU. However, the CJEU found the CFSP legal basis for the EU-Mauritius agreement to be appropriate.[307]

Moreover, in the *Al-Qaeda Sanctions* case from 2012, the European Parliament challenged the Council's use of a CFSP Common Position 2002/402 under Title V TEU, in conjunction with article 215(2) TFEU, to enact restrictive measures directed against certain persons and entities associated with the Al-Qaeda network.[308] It argued that the Council Regulation (EU) No 1286/2009 should have been adopted instead under article 75 TFEU as part of the AFSJ, which is also a legal basis devoted to sanctions for the freezing of funds, and provides for the ordinary legislative procedure.[309] In other words, the European Parliament argued that article 75 TFEU should have been the legal basis for the anti-terrorist sanctions rather than article 215(2) TFEU.

However, the CJEU rejected the European Parliament's argument. The Court ruled that article 215(2) TFEU constitutes the appropriate legal basis for the contested measures directed to persons and entities implicated in acts of terrorism who, having regard to their activities globally and to the international dimension of the threat they pose, affect fundamentally the Union's external activity.[310] Thus, the Parliament's main argument attempting to distinguish between "internal" and "external" terrorism was rejected by the CJEU.[311] The CJEU has indeed retained the international dimension of international terrorism as a criterion for choosing between the legal basis linked to the CFSP (Art. 215 TFEU) and the AFSJ legal basis (Art. 75 TFEU) for a regulation imposing a freeze on funds. Although the CJEU held that the combating of terrorism and its financing may well be among the objectives of the AFSJ, it concluded that the objective of combating international terrorism and its financing in order to preserve international peace and security corresponds, nevertheless, to the objectives of the Treaty provisions on external action by the Union.[312] As terrorism constitutes a threat to peace and international security, the international dimension is clear enough to consider the CFSP to be the appropriate legal basis of the restrictive measures. Also, the fact that it was a regulation

[307] Ibid., paragraphs 44-45
[308] "Judgment of the Court (Grand Chamber) of 19 July 2012. European Parliament v Council of the European Union. Case C-130/10," paragraph 12, EUR-Lex, accessed 23 November 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62010CJ0130
[309] Ibid., paragraph 34
[310] Ibid., paragraph 78
[311] Ibid., paragraph 74
[312] Ibid., paragraphs 61-63

implementing a UN Security Council Resolution facilitated the demonstration of the international dimension.

When it comes to the cyber sanctions regime however, it is an autonomous decentralised sanctions regime established by the EU. Indeed, it does not implement any UN Security Council Regulation. With regards to cyber malicious acts, the clash of border between CFSP and AFSJ could be raised. Indeed, under AFSJ, article 83 TFEU allows for sanctions in the case of criminal offences such as computer crime and organised crime.[313] Therefore, with regards the cyber sanctions regime, the question could be raised whether it has been inappropriately based on article 215 TFEU, as part of CFSP. This would solve the CFSP decision-making process challenge the EU is confronted with.

Hence, the real question with regards the clash between CFSP and AFSJ concerns the "external" element of the cyber sanctions regime of 2019. Does the mere fact that the perpetrator of the malicious cyber-attack was supported by a person acting outside of the Union, which constitutes this "external" dimension, allow to disqualify the AFSJ and reject the scope of application of article 83 TFEU? In other words, can article 83 TFEU, as part of AFSJ, cover cyber sanctions with this external dimension?

The problem lies with the fact that there may be several situations where the external element of a cyber-attack is met. According to the cyber sanctions regime, the external element is met if the cyber-attack: (1) originates from outside the Union, (2) uses infrastructure outside the Union, (3) is carried out by any person or entity established outside the Union, (4) or is carried out with the support of a person operating outside the Union.[314] As for the three first situations, the external element is clearly established.

However, for the last one, the external element will be met if the perpetrator of the attack operated it under the control of a foreign company or government. In this case, the perpetrator could be inside the territory of the EU and get the support of a person established outside of the EU. The external element is linked to the support coming from outside of the EU. Yet, the cyber-attack could originate from inside the EU. This situation could open the border clash between the CFSP and the AFSJ. Indeed, it could be argued that the fact that the perpetrator of the malicious cyber-attack was supported by a person acting outside of the Union is not enough

[313] "Consolidated Version of the Treaty on The Functioning of the European Union signed on 13 December 2007," op. cit., article 83, paragraphs 1 and 2.
[314] "Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States,". op. cit.

as to meet the external dimension of a cyber malicious act. Thus, it could be considered a computer crime falling under the scope of the AFSJ.

If during the legal attribution level, the cyber malicious act is classified as a cybercrime instead of a cyber-attack, then the cyber malicious act will fall under the scope of article 83 TFEU of the AFSJ. It could happen that a same cyber malicious act could be classified differently, depending on the forensic capabilities, either as a cybercrime or a cyber-attack.[315] As the criteria are unclear, it might be a question of interpretation as to whether the cyber malicious act is more of a cybercrime than a cyber-attack.

However, as for terrorism in the *Al-Qaeda* case, the cyber-attacks constitute a threat to international security. Indeed, the Council stated that the EU upholds the international consensus that existing international law is applicable to cyberspace and emphasised that respect for international law, especially from the United Nations Charter, is essential to maintaining peace and stability.[316] Therefore, the cyber sanctions regime achieves one of the CFSP objectives laid down under article 21 TEU, namely to maintain international peace and security.

Based on the CJUE's caselaw, it seems very unlikely that the cyber sanctions regime will be challenged arguing that it should have been adopted under AFSJ on the basis of article 83 TFEU. First, the cyber sanctions regime is part of EU's cyber diplomacy. Second, no precedent can support this argument. The *Al-Qaeda* case suggested that the scope of application of article 75 TFEU to EU anti-terrorists sanctions with an external dimension is likely to be extremely limited.[317] Third, only one situation of cyber-attack could be considered a computer crime. So, by analogy, the scope of application of article 83 TFEU to cyber sanctions with an external dimension is nearly impossible.

Still, the idea of such a possibility should not be overlooked. This would be a solution so as to overcome the intergovernmental character issue inherent to CFSP, thus to the cyber sanctions regime. Subsequently, it would maybe allow for better effectiveness in the process of adopting sanctions against cyber-attacks as the ordinary legislative procedure would be in place. The unanimity requirement would be side-lined. Hence, the Cyber Diplomacy Toolbox's effectiveness, and the cyber sanctions regime, could be enhanced.

[315] Bendiek, and Schulze, op. cit., 11.
[316] Ibid.
[317] Craig, and De Búrca op. cit., 348.

Nevertheless, such a solution is only theoretical. The intergovernmental nature of CFSP still represents a major limit in the context of cyber cold war and to the effectiveness of the EU cyber sanctions regime.

Conclusions

This thesis has analysed the legal framework for the new cyber sanctions regime stemming from Decision 2019/797 and Regulation 2019/796. It concludes that new EU cyber sanctions regime is an autonomous and decentralised sanctions regime which follows the traditional two-step procedure stemming from articles 29 TEU and 215 TFEU. In compliance with the principle of legal certainty, the grounds for listing are similar to other restrictive measures' regimes. Nevertheless, and notably, the cyber sanctions regime consists of one of the few EU horizontal sanctions regime. Thus, the novelty from this sanctions regime stems from the notion of cyber-attack having significant effect which constitutes an external threat to the Union or its Member States.

Indeed, the definition of cyber-attack is unique and has been adopted specifically for the purpose of the cyber sanctions regime. However, the criteria for listing linked to the notion of "significant effect" of a cyber-attack are broad and unclear. As the criteria are imprecise, it gives the Council some arbitrary power in assessing whether the cyber-attack has significant effect to the detriment of legal certainty. Unlike other EU sanctions regime, this is a difficulty specific to the notion of cyber-attacks due to its inherent anonymity character. Therefore, the legal attribution represents an important challenge as being an indispensable and preliminary step before adopting a cyber sanction.

This thesis has demonstrated that the intergovernmental nature of the EU's CFSP represents an important obstacle to the effectiveness of the EU cyber sanctions regime in the cyberwar context. The Cyber Diplomacy Toolbox is a CFSP instrument developed through the EU's diplomacy strategy of resilience against the increasing of cyber-attacks. As part of the Cyber Diplomacy Toolbox, the cyber sanctions regime, which followed the two-step approach stemming from article 29 TEU and article 215 TFEU, is intrinsically linked to the intergovernmental nature of the CFSP. The CFSP is an area where member states retain their sovereign prerogatives. Thus, each member state has a veto on every decision which makes it difficult to achieve a common position. Consequently, this has a direct impact in the decision-making of the cyber sanctions by the Council; especially during the policy of attribution. For the EU to enlist targeted persons found responsible for the cyber-attacks in question, the Council needs to take a decision at unanimity. The unanimity requirement represents an important obstacle to the collective attribution. It does not seem so surprising if only two packages of cyber sanctions have been adopted by the EU. Getting all Member States to agree

in an area where national interests are at stake is perilous. The policy of attribution cannot be effective as solely dependent on the intergovernmental character and decision-making of the CFSP.

The thesis has assessed that the collection of forensic evidence, necessary to support a cyber sanction, constitutes an important legal challenge for the EU. Indeed, as the EU has no real operator role when it comes to collect substantiated evidence, depending on intelligence capabilities of other actors, it reveals the loophole of the cyber sanctions regime. The decision targeting the persons responsible for the cyber-attacks must disclose the reasons for listings alongside with substantial evidence. However, these decisions are subject to the judicial high standard set by the CJEU. They must respect the fundamental rights, in particular right to an effective remedy and to a fair trial. Yet, the Council might not be willing to disclose confidential information and evidence to the targeted person as it could compromise the security of the EU and its member states. Therefore, it is up for the CJEU to strike a balance between the right to effective judicial protection and the security of the EU or its member states. The CJEU's scrutiny with regards decision enlisting the targeted persons is high. The requirement of substantiated by evidence the reasons for targeting persons is even harder to reach with the anonymity character inherent to cyber-attacks. Hence, the Council will lose cases of cyber sanctions before the CJEU's judicial review. This appears to be an important hurdle to the effective contribution of the cyber sanctions regime to the EU sanctions regime.

Finally, the question regarding the border clash between the CFSP and the AFSJ regarding cyber-attacks could be a solution to overcome the intergovernmental character issue inherent to the CFSP. As theoretically falling under the AFSJ, the unanimity requirement would be side-lined for the qualified-majority voting. However, challenging the cyber sanctions regime by arguing it should be based on the AFSJ rather than the CFSP seems highly unreliable and unfeasible. Indeed, the analysis has shown that only one situation could fall under article 83 TFEU of the AFSJ. Where the perpetrator of the malicious cyber-attack was supported by a person acting outside of the Union. The external element, necessary to the CFSP, is linked to the support coming from outside of the EU. Yet, the cyber-attack could originate from inside the EU. Therefore, it this situation be considered not enough as to meet the external dimension of a cyber-attack and consequently to be defined as a computer crime falling under the scope of the AFSJ. Therefore, such a solution to circumvent the intergovernmental nature of CFSP and consequently to enhance the cyber sanctions regime's effectiveness appears illusory.

List of bibliography

Treaties and legislation

1. "Budapest Convention on Cybercrime of the Council of Europe." ETS 185. 23 November 2001. https://rm.coe.int/1680081561
2. "Charter of Fundamental Rights of the European Union." OJ C 326. 26 October 2012. http://data.europa.eu/eli/treaty/char_2012/oj
3. "Charter of the United Nations." 26 June 1945. https://www.un.org/en/about-us/un-charter/full-text
4. "Consolidated Version of the Treaty establishing the European Community." OJ C 325. 24 December 2002. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12002E%2FTXT
5. "Consolidated Version of the Treaty on European Union signed on 13 December 2007." *OJ C 326/13. 26 October 2012.* https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0023.02/DOC_1&format=PDF
6. "Consolidated Version of the Treaty on The Functioning of the European Union signed on 13 December 2007." *OJ C 326/47. 26 October 2012.* https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2008:115:0013:0045:en:PDF
7. "Council conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")." Council of the European Union. OJ 10474/17. 19 June 2017. https://data.consilium.europa.eu/doc/document/ST-10474-2017-INIT/en/pdf
8. "Council conclusions on malicious cyber activities." Council of the European Union. OJ 7925/18. 16 April 2018. http://data.consilium.europa.eu/doc/document/ST-7925-2018-INIT/en/pdf
9. "Council Decision (CFSP) 2018/1544 of 15 October 2018 concerning restrictive measures against the proliferation and use of chemical weapons." Council of the European Union. OJ L 259. 16 October 2018. http://data.europa.eu/eli/dec/2018/1544/oj
10. "Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States." Council of the European Union. OJ L 129I. 17 May 2019. http://data.europa.eu/eli/dec/2019/797/oj
11. "Council Decision (CFSP) 2020/1127 of 30 July 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member

States." Council of the European Union. OJ L 246. 30 July 2020. http://data.europa.eu/eli/dec/2020/1127/oj

12. "Council Decision (CFSP) 2020/1537 of 22 October 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States." Council of the European Union. OJ L 351I. 22 October 2020. http://data.europa.eu/eli/dec/2020/1537/oj
13. "Council Decision (CFSP) 2020/1999 of 7 December 2020 concerning restrictive measures against serious human rights violations and abuses." Council of the European Union. OJ L 410I. 7 December 2020. http://data.europa.eu/eli/dec/2020/1999/oj
14. "Council Implementing Regulation (EU) 2020/1125 of 30 July 2020 implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States." Council of the European Union. OJ L 246. 30 July 2020. http://data.europa.eu/eli/reg_impl/2020/1125/oj
15. "Council Regulation (EEC) No 877/82 of 16 April 1982 suspending imports of all products originating in Argentinap." Council of the European Union. OJ L 102. 16 April 1982. http://data.europa.eu/eli/reg/1982/877/oj
16. "Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States." Council of the European Union. OJ L 129I. 17 May 2019. http://data.europa.eu/eli/reg/2019/796/oj
17. "Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA." European Parliament and Council of the European Union. OJ L 218. 14 August 2013. http://data.europa.eu/eli/dir/2013/40/oj
18. "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union." European Parliament and Council of the European Union. OJ L 194. 19 July 2016. http://data.europa.eu/eli/dir/2016/1148/oj
19. "Draft Council conclusions on Cyber Diplomacy." Council of the European Union. OJ 6122/15, 11 February 2015. https://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf
20. "Draft Council conclusions on the EU's Cybersecurity Strategy for the Digital Decade." Council of the European Union. OJ 6722/21. 9 mars 2021. https://data.consilium.europa.eu/doc/document/ST-6722-2021-INIT/en/pdf

21. “Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities.” Council of the European Union. OJ 13007/17. 9 October 2017. https://data.consilium.europa.eu/doc/document/ST-13007-2017-INIT/en/pdf
22. “Joint communication to the European parliament, the European council and the council - Increasing resilience and bolstering capabilities to address hybrid threats.” European Commission and High Representative of the Union for Foreign Affairs and Security Policy. JOIN(2018) 16 final. 13 June 2018. https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:52018JC0016
23. “Non-Paper: Developing a Joint EU Diplomatic Response Against Coercive Cyber Operations.” Council of the European Union. 5797/6/16. 19 May 2016. http://statewatch.org/news/2016/jul/eu-council-diplomatic-response-cyber-ops-5797-6-16.pdf
24. “Rules of procedure of the General Court.” OJ L 105. 23 April 2015. http://data.europa.eu/eli/proc_rules/2015/423/oj

Official documents and reports

1. “An area of freedom, security and justice: general aspects.’’ European Parliament. *Fact Sheets on the European Union*, 2022. Accessed 17 November 2022. https://www.europarl.europa.eu/factsheets/en/sheet/150/an-area-of-freedom-security-and-justice-general-aspects
2. "Council Conclusions on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU." Council of the European Union, 20 November 2017. Accessed 14 December 2022. https://www.consilium.europa.eu/media/31666/st14435en17.pdf
3. “Cyber-attacks: Council is now able to impose sanctions.” Council of the European Union. *Press release*, 17 May 2019. https://europa.eu/!yp76kW
4. “Declaration by the High Representative on behalf of the EU on respect for the rules-based order in cyberspace.*”* Council of the European Union. *Press release*, 12 April 2019. https://europa.eu/!rm83yB
5. “Declaration by the High Representative on behalf of the EU on the alignment of certain countries concerning restrictive measures against cyber-attacks threatening the Union or its

Member States." Council of the European Union. *Press release*, 7 June 2022. https://europa.eu/!MBbph7

6. ‘‘Déclaration de Madame, ministre des armées, sur la stratégie cyber des armées.’’ Paris, January 18, 2019. Accessed 4 October 2022. https://www.vie-publique.fr/discours/269137-florence-parly-18012019-strategie-cyber-des-armees-cyberdefense
7. "Draft articles on Prevention of Transboundary Harm from Hazardous Activities." International Law Commission (ILC). *2001 Yearbook of the ILC.* https://legal.un.org/ilc/texts/instruments/english/commentaries/9_7_2001.pdf
8. "ENISA Threat Landscape 2022." European Union Agency for Cybersecurity. November 2022. https://doi.org/10.2824/764318
9. "EU INTCEN Intelligence Analysis Centre." EU INTCEN. *Fact Sheet*, 5 February 2015. Accessed 21 November 2022. https://www.statewatch.org/media/documents/news/2016/may/eu-intcen-factsheet.pdf
10. "EU sanctions two individuals and one body over 2015 Bundestag hack." Council of the European Union. *Press release*, 22 October 2022. https://europa.eu/!CJ48PC
11. "European Commission President Jean-Claude Juncker. State of the Union Address." 13 September 2017. https://ec.europa.eu/commission/presscorner/api/files/document/print/en/speech_17_3165/SPEECH_17_3165_EN.pdf
12. "Extension of cyber sanctions regime to 18 May 2025." Council of the European Union. *Press release*, 16 May 2022. https://europa.eu/!qfDkPr
13. "Foreign policy: aims, instruments and achievements." European Parliament. *Fact Sheets on the European Union*, 2022. Accessed 17 November 2022 https://www.europarl.europa.eu/factsheets/en/sheet/158/foreign-policy-aims-instruments-and-achievements
14. "Frequently asked questions: Restrictive measures (sanctions)." European Commission, 26 February 2022. Accessed 9 November 2022. https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_1401
15. "General Framework for EU Sanctions." Office of the European Union. *EUR-Lex*, 9 October 2020. Accessed 9 November 2022. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:25_1
16. "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security." United Nations Secretary General. 22 July 2015. A_70_174-EN.pdf

17. ‘’Harnessing the Power of Trust.’’ European Cyber Agora. *ECA Brussels Communiqué 2022*, 2022. Accessed 21 November 2022. https://www.microsoft.com/en-eu/cyber-agora/
18. “Recent cyber-attacks and the EU's cybersecurity strategy for the digital decade.” European Parliament. *Plenary*, 1 June 2021. https://www.europarl.europa.eu/RegData/etudes/ATAG/2021/690639/EPRS_ATA(2021)690639_EN.pdf
19. ”Resilience, Deterrence and Defence: Building strong cybersecurity in Europe.” European Commission. *State of the Union*, 2017. www.consilium.europa.eu/media/21480/cybersecurityfactsheet.pdf
20. “Restrictive measures (sanctions).” Office of the European Union. *EUR-Lex*, 28 July 2021. Accessed 9 November 2022. https://eur-lex.europa.eu/EN/legal-content/glossary/restrictive-measures-sanctions.html
21. “Top cyber threats in the EU.” European Council, and Council of the European Union. *Infographic*, 27 October 2022. https://europa.eu/!cw89Pv
22. “Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups.” U.S. Department of the Treasury. *Press Releases*, 13 September 2019. https://home.treasury.gov/news/press-releases/sm774
23. “Treasury Targets North Korea for Multiple Cyber-Attacks.*”* U.S. Department of the Treasury. *Press Releases*, 6 September 2018. https://home.treasury.gov/news/press-releases/sm473

Caselaw

1. “Award of the Permanent Court of Arbitration of 4 April 1928. Island of Palmas case (Netherlands, USA).” Reports Of International Arbitral Awards. Accessed 14 December 2022. https://legal.un.org/riaa/cases/vol_II/829-871.pdf
2. “Judgment of the Court (Grand Chamber) of 3 September 2008. Yassin Abdullah Kadi and Al Barakaat International Foundation v Council of the European Union and Commission of the European Communities. Joined cases C-402/05 P and C-415/05 P.” EUR-Lex. Accessed 23 November 2022. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A62005CJ0402

3. "Judgment of the Court (Grand Chamber) of 18 July 2013. European Commission and Others v Yassin Abdullah Kadi. Joined Cases C-584/10 P, C-593/10 P and C-595/10 P." EUR-Lex. Accessed 23 November 2022. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A62010CJ0584
4. "Judgment of the Court (Grand Chamber) of 19 July 2012. European Parliament v Council of the European Union. Case C-130/10." EUR-Lex. Accessed 23 November 2022. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62010CJ0130
5. "Judgment of the Court (Grand Chamber) of 24 June 2014. European Parliament v Council of the European Union. Case C-658/11." EUR-Lex. Accessed 16 December 2022. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62011CJ0658
6. "Judgment of the Court (Grand Chamber) of 28 March 2017. PJSC Rosneft Oil Company, formerly OJSC Rosneft Oil Company v Her Majesty's Treasury, Secretary of State for Business, Innovation and Skills, The Financial Conduct Authority. Case C-72/15." EUR-Lex. Accessed 23 November 2022. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62015CA0072
7. "Judgment of the International Court of Justice of 4 April 1949. Corfu Channel case." ICJ Reports. Accessed 18 November 2022. https://www.icj-cij.org/public/files/case-related/1/001-19490409-JUD-01-00-EN.pdf

Books and Journal articles

1. Bendiek, Annegret. "The European Union's Foreign Policy Toolbox in International Cyber Diplomacy." *Cyber, Intelligence, and Security* 2, 3 (2018): 57-70.
2. Bendiek, Annegret., and Matthias Schulze. "Attribution: a major challenge for EU cyber sanctions. An analysis of WannaCry, NotPetya, Cloud Hopper, Bundestag Hack and the Attack on the OPCW." *SWP Research Paper* 11 (2021): 5-42. doi:10.18449/2021RP11
3. Bertrand, Brunessen. ''Chronique Droit européen du numérique. La nouvelle approche de la cybersécurité européenne.'' *Revue Trimestrielle Droit Européen* 1 (2021): 155-160. https://www.dalloz.fr/documentation/Document?id=RTDEUR/CHRON/2021/0112
4. Bertrand, Brunessen. "La souveraineté numérique européenne : une « pensée en acte » ?" *Revue Trimestrielle Droit Européen* 2 (2021): 249-278. https://www.dalloz.fr/documentation/Document?id=RTDEUR/CHRON/2021/0394

5. 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, 2 (2020): 3-9.
6. Cammilleri, Anne. ‘’L’espace numérique : un patchwork européen renouvelé par le calcul quantique.’’ *Revue du droit de l’Union européenne* 2 (2022): 31-56.
7. Chauvel, Louis-Marie., and Anne Hamonis. ‘‘Chronique Action extérieure de l'UE. La diversification des régimes thématiques de mesures restrictives.’’ *Revue Trimestrielle Droit Européen* 3 (2019): 746-751. https://www.dalloz.fr/documentation/Document?id=RTDEUR/CHRON/2019/0631
8. Cirlig, Carmen-Cristina. “Cyber defence in the EU. Preparing for cyber warfare?” *European Parliamentary Research Service* PE 542.143 (2014): 1-10.
9. Craig, Paul., and Gráinne De Búrca. *EU Law. Text, Cases, and Material.* Oxford: Oxford University Press, 2015.
10. De Maison Rouge, Olivier. ‘’L’intégration de contre-mesures économiques dans la prévention des cyberattaques. Le règlement (UE) 2019/796 du 17 mai 2019 et décision (PESC) 2019/797 du 17 mai 2019.’’ *Dalloz IP/IT* (2019): 574-577.
11. Deschaux-Dutard, Delphine. ‘’L'Union européenne, une cyberpuissance en devenir ? Réflexion sur la cyberdéfense européenne.’’ *Revue internationale et stratégique* 1, 117 (2020): 18-29. https://doi.org/10.3917/ris.117.0018
12. D’Elia, Danilo. ‘’La cybersécurité : de la représentation d’un bien public à la nécessité d’une offre souveraine.’’ *Sécurité et stratégie* 19, 2 (2015): 72-80. https://doi.org/10.3917/sestr.019.0072
13. Doutriaux, Yves. “La boussole stratégique et l’invasion de l’Ukraine par la Russie.“ *Revue de l’Union européenne* 661 (2022): 468-475.
14. Giantas, Dominika. “Cybersecurity in the EU: Threats, Frameworks and future perspectives.” *Laboratory of Intelligence and Cyber-security* 1 (2019): 3-40. https://www.researchgate.net/publication/335909463_Cybersecurity_in_the_EU_Threats_frameworks_and_future_perspectives
15. Ivan, Paul. “Responding to cyberattacks: Prospects for the EU Cyber Diplomacy Toolbox.” Discussion Paper, *Europe in the world programme* (2019): 3-16. http://aei.pitt.edu/97071/1/pub_9081_responding_cyberattacks.pdf.
16. Kapsokoli, Eleni. “Sanctions and Cyberspace: The Case of the EU’s Cyber Sanctions Regime.” *Academic Conferences International Limited* (2021): 492-498. https://doi.org/10.34190/EWS.21.029

17. Miadzvetskaya, Yuliya. “Chapter 12: Challenges of the cyber sanctions regime under the common foreign and security policy (CFSP).” In *Security and Law: Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security*, A. Vedder, J. Schroers, C. Ducuing, P. Valcke, 277-298. Cambridge: Cambridge University Press, 2019.
18. Miadzvetskaya, Yuliya. “Cyber sanctions: towards a European Union cyber intelligence service?” *College of Europe Policy Brief* 1, 21 (2021): 1-5. http://aei.pitt.edu/id/eprint/103385
19. Miadzvetskaya, Yuliya., and Ramses A. Wessel. ‘’The Externalisation of the EU’s Cybersecurity Regime: The Cyber Diplomacy Toolbox.’’ *European Paper* 7, 1 (2022): 413-438. https://ssrn.com/abstract=4199627
20. Moret, Erika., and Patryk Pawlak. “The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime?” *European Union Institute for Security Studies (EUISS)* (2017): https://doi.org/10.2815/399444
21. Moynihan, Harriet. “The Application of International Law to State Cyberattacks. Sovereignty and Non-intervention.” Research Paper. *International Law Programme* (2019): 2-59
22. Nye, Joseph S. “Deterrence and Dissuasion in Cyberspace.” *International Security* 41, 3 (2017): 44–71. https://doi.org/10.1162/ISEC_a_00266
23. Pawlak, Patryk., and Thomas Biersteker. ‘’Guardian of the Galaxy: EU cyber sanctions and norms in cyberspace.’’*Chaillot Paper* 155 (2019): 1-102. https://www.iss.europa.eu/sites/default/files/EUISSFiles/cp155.pdf
24. Pawlak, Patryk., Eneken Tikk, and Mika Kerttunen. “Cyber conflict encoded: the EU and conflict prevention in cyberspace.” Conflict series, *European Union Institute for Security Studies*, 7 (2020): 1-8. https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%207_Cyber.pdf
25. Schmitt, Michael N. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, 2017. https://doi.org/10.1017/9781316822524
26. Shooter, Simon. “Cyber Security and the EU: regulating for network security.” *Bird& Bird* (2013): 1-2.
27. Watin-Augouard, Marc., and Guillaume Klossa. “Making cybersecurity the cornerstone of European Digital Sovereignty.” 28 Recommendations for the French Presidency of the

Council of the European Union on Digital Security and Regulation, *Agora FIC* (2021): 1-65. https://agora-fic.com/wp-content/uploads/2022/08/Agora_FIC_2021_White_Paper_Cybersecurity_Europe_EN.pdf

Newspaper Articles

1. Harding Luke. “”Ukraine Hit By “Massive” Cyber-Attack on Government Websites.” *The Guardian*, January 14, 2022. https://www.theguardian.com/world/2022/jan/14/ukraine-massive-cyber-attack-government-websites-suspected-russian-hackers
2. Reynaud Florian, and Adam Louis. ‘’Cyberattaque contre l’hôpital de Corbeil-Essonnes : ce que l’on sait sur les données diffusées.’’ *Le Monde*, Septembre 26, 2022. https://www.lemonde.fr/pixels/article/2022/09/26/apres-la-cyberattaque-contre-l-hopital-de-corbeil-essonnes-ce-que-l-on-sait-sur-les-donnees-diffusees_6143245_4408996.html
3. Untersinger Martin, and Leloup Damien. ‘’ « Affaire Pegasus » : un an après, le crépuscule de NSO Group.’’ *Le Monde*, July 18, 2022. https://www.lemonde.fr/pixels/article/2022/07/18/affaire-pegasus-un-an-apres-le-crepuscule-de-nso-group_6135168_4408996.html

Websites

1. ‘’Europe has no strategy on cyber sanctions.” Soesanto, Stefan. Cybersecurity and deterrence. Lawfare Institute in Cooperation with Brookings. Accessed 10 October 2022. https://www.lawfareblog.com/europe-has-no-strategy-cyber-sanctions
2. “Israel Launches $24M Program to Strengthen Cyber Industry.” Talk, Hyvor. IsraelDefense. Accessed 21 November 2022. https://www.israeldefense.co.il/en/node/35291
3. “Italy resisting EU push to impose sanctions over cyberattacks.” Guarascio Francesco. Reuters. Accessed 10 November 2022. https://www.reuters.com/article/us-italy-russia-sanctions-idUSKCN1MM2CP
4. ‘’Si vis cyber pacem, para sanctiones: the EU Cyber Diplomacy Toolbox in action.’’ De Tomas Colatin, Samuele. NATO Cooperative Cyber Defence Centre of Excellence. Accessed 4 October 2022. https://ccdcoe.org/library/publications/si-vis-cyber-pacem-para-sanctiones-the-eu-cyber-diplomacy-toolbox-in-action/

5. “The Development of the EU Cyber Security Strategy and its Importance.” Vela, Jorida. FINABEL. Accessed 3 November 2022. https://finabel.org/info-flash-the-development-of-the-eu-cyber-security-strategy-and-its-importance/
6. “The Untold Story of NotPetya, the Most Devastating Cyberattack in History.” Greenberg, Andy. Wired. Accessed 10 November 2022. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Abstract

The EU's diplomatic cyber strategy is an important demonstration of its concern and responsiveness with regards disastrous cyber-attacks. In light of the new threats cyber-attacks represent for the economy and democracy, the EU institutions and member states decided to establish a cyber resilience instrument as part of its CFSP. Therefore, in 2017 the Cyber Diplomacy Toolbox was adopted with the aim of ensuring stable, peaceful and secure cyberspace in the EU. Among the five instruments provided by the Cyber Diplomacy Toolbox, the most notable is the legal framework for restrictive measures against cyber-attacks stemming from Decision 2019/797 and Regulation 2019/796.

Undeniably, considering the cyberwar context, the Cyber Diplomacy Toolbox, and in particular the cyber sanctions regime, appears to be a most needed instrument within the EU's cyber deterrence strategy. However, its contribution is merely symbolic. This ensues mostly from both the CFSP's intergovernmental nature and the anonymous character of cyberspace which represent a hurdle to the adoption of a cyber sanction.

Key words: Cyber Diplomacy Toolbox, cyber sanctions regime, restrictive measures, cyber-attacks, CFSP.

Summary

The topic of this thesis is “The EU Cyber Diplomacy Toolbox: impact on the EU sanctions regime”. The Cyber Diplomacy Toolbox provides for a legal framework for restrictive measures against cyber-attacks. This new autonomous sanctions regime raises legal questions with regards its impact on the general sanctions regime. The aim of the thesis is to determine whether the EU cyber sanctions regime within the Cyber Diplomacy Toolbox contributes distinctively to the EU sanctions regime given its legal framework and the intergovernmental nature of the CFSP.

Since the Covid-19 pandemic, cybersecurity has been at the heart of debates and has become a major issue for companies in all sectors. Indeed, the introduction of widespread remote working has contributed to the acceleration of the digital transformation. Yet, the digitalisation of our societies and economies involves new types of risks, namely cyberattacks. They have drastically increased in the EU in 2020 and 2021, especially ransomware attacks. Therefore, the EU developed its own diplomatic strategy following its will to cyber response, resilience and deterrence. The EU diplomatic strategy led to the adoption of the Cyber Diplomacy Toolbox and in its continuity an autonomous sanctions regime in 2019, namely the new EU cyber sanctions regime. Their analysis is necessary to demonstrate that the Cyber Diplomacy Toolbox is a symbolic input on the EU sanctions regime.

Moreover, the thesis focuses on the limits faced by the cyber sanctions regime. Inasmuch as the cyber sanctions regime is a CFSP measure, the decision to adopt a sanction is inevitably difficult to achieve. The CFSP is based on an intergovernmental decision-making procedure, where the Member States detain a veto right. Yet, the border clash between the CFSP and the AFSJ might not be a feasible solution to overcome this intergovernmental character of CFSP. Moreover, the difficulty of collecting evidence for reasons of the anonymity nature of cyberspace. Especially, to support a decision adopting a sanction before the CJEU’s judicial review. Therefore, the evidence collection appears to be a loophole diminishing the legitimacy of the cyber sanctions regime. The thesis concludes that the contribution of the EU cyber sanctions regime on the EU sanctions regime is symbolic.