POLITICON : Jurnal Ilmu Politik Vol.5 No.1 ; Hal 29 – 58
Website : http://journal.uinsgd.ac.id/index.php/politicon
ISSN : 2685-6670 (Online)

Establishment of The Cyber Diplomacy Toolbox (CDT) as a Joint Diplomatic Response to the European Union Against the Threat of Cyber Attack activity

Miftahul Khausar[1], Abdul Rivai Ras[2]
[1,2]European Studies, School of Strategic and Global Studies, University of Indonesia, Indonesia
*Corresponding author E-mail: miftahul.khausar@ui.ac.id

Received: January 10, 2023; Revised: March 5, 2023; Approved: March 30, 2023

ABSTRACT

In June 2017, the European Union increased its vigilance regarding Cyber Attack/Cybercrime issues by deciding and supporting the establishment of a framework for EU joint diplomacy on cyber threat issues, called “The EU Cyber Diplomacy Toolbox (CDT) because the cyber threat has harmed its member countries. Therefore, this study will analyze the European Union's Cyber Security strategy, especially looking at the Formation of CDT as a Joint Diplomatic Response of the European Union against the threat of Cyber Attack activity. The research method used in this study is a qualitative method using primary data sources obtained directly from the official website of the European Union and secondary data in the form of literature review. This research is analyzed using International Security Theory and Cyber Diplomacy Concepts.

Keywords: European Union(EU), International Security, Cyber Diplomacy, Cyber Security, Cyber Attack

INTRODUCTION

The Digital Age (also known as The Information Age) which is marked by the development of Information and Communication Technology (ICT) is currently bringing major changes from the Individual level to the Global Level (Hamonangan. I, 2020). This indicates a change in the pattern of information movement, in this case using the term information revolution, as seen from the increasing number of forms of electronic communication, most of which are still not regulated in existing regulations. The faster the delivery of information such as news on an issue and the easier access for the public to receive information from becomes a big challenge that is so complex for state administrators. Technological developments heralded as ushering in a new era of transparency are technologies that countries can use to increase their oversight needs, reconnaissance, and communication itself (Potter, 2002).

Various kinds of problems have also begun to develop in electronic media in computer networks, in this case, known as the Cyber World or Cyberspace. The fact that most of the telecommunications infrastructure is owned by the private sector is a fact that is little known (Knapp, 2009). This makes it difficult for the state to provide overall supervision and prosecution. Problems such as Cyber Crime or Cyber Crime have the potential to threaten security at the individual, institutional, or state level including the European Union. Cyber-attacks against the European Union and its member countries have occurred frequently, but the actions taken have only been limited to identifying the perpetrators, whether state or private, from outside the European Union area, but there have not been any steps to take action against these perpetrators. If the European Union does not have a solution to these problems it will most likely make the EU weak in the future (Sliwinski, 2014)

European Union Member States have long been committed to the Common Foreign and Security Policy (CFSP) which has an important role in external relations and the world order scheme referred to by the European Union (EU) (Fahmi, 2008). The CFSP which is the European Security and Defense Policy aims to strengthen the EU's external capabilities to act through the development of civil and military capabilities in Conflict Prevention and Crisis Management. To influence policies that violate international law, human rights, or policies that do not respect the rule of law or democratic principles, the EU has devised sanctions of a diplomatic or economic nature(European External Action Service (EEAS), 2019).

The CFSP represents the EU security community which upholds Mutual security solidarity and the awareness that an attack on one member will have a direct impact on all (Howorth & Menon, 2005). In addition, the CFSP is intergovernmental in nature, in which each member state has the authority in determining EU policies related to defense and security issues, including the imposition of diplomatic and economic sanctions against anyone who threatens the defense and security of EU member states. The policy of imposing sanctions in the European Union has become a legal and procedural formalism that has contributed to facilitating the legalization process, even the post-Lisbon CFSP has focused on the use of sanctions as a special representation of the form of legalized instruments. (Cardwell, 2015). Many sanctions have been issued by the European Union against countries that directly threaten the defense and security of its Members.

In practice, the EU seeks to maintain the security and defense of various sectors, including cyber threats or cybercrime, the EU has enhanced its cybersecurity strategy to prevent, deter and respond to cybercrime threats. In June 2017, the EU raised its awareness regarding the issue of Cybercrime by deciding and supporting the establishment of a framework for joint EU diplomacy on cyber threat issues, called The EU Cyber Diplomacy Toolbox (CDT) in practice the framework allows the EU and its member states to use Action CFSP, to prevent, limit, respond to and act against Cybercrime or CyberAttack activities that target the integrity and security of the EU and its Member countries(The Council of the European Union, 2020). Sanctions are also one of the options in The EU Cyber Diplomacy Toolbox (CDT) regarding cyber threats that are increasingly prevalent in the Digital Age

Cyberattacks have several times caused huge losses to the European Union. Therefore, the European Union should have a specific strategy in responding to these cybercrime incidents that threaten its Member States. The increasing number of cyber attacks in the European Union, be it against individuals, institutions, or countries, requires the European Union to have special laws or rules as protection. Legal protection is an illustration of the functioning of the legal function to realize legal objectives, namely justice, benefit, and legal certainty. Legal protection a protection given to legal subjects in accordance with the rule of law, both preventive (preventive) and repressive (coercive) forms, both written and unwritten in order to enforce legal regulations (Hadis, 2020). Therefore, as an initial step for this protection, the European Union has created a joint framework specifically to discuss Cyber issues which can later produce a legal product or sanctions.

Cyber sanctions are part of the EU's Cyber Diplomacy Toolbox (CDT) which seeks to prevent and respond to malicious cyberattacks that have a significant impact on the EU. This framework was adopted in May 2019 under Council Decree (CFSP) 2019/797 and Council Regulation (EU) 2019/796 , and is reviewed by the Council annually. This allows the EU to sanction persons and entities deemed to be involved in major cyberattacks that threaten the EU or its Member States by imposing asset freezes or travel bans on those listed in the Council's legal acts. The EU can also target those involved in attempted cyberattacks with potentially significant effect.

The CDT includes many instruments related to cyberspace activities in the European region to develop signaling and reactive capacity in the European Union. In addition, one of the instruments that is also very important from the CDT is the imposition of sanctions that aim to influence the behavior of potential attackers, taking into account the needs and proportionate responses of EU member states (Moret & Pawlak, 2017). The challenge for the EU after that is the implementation of these provisions in the form of a foreign policy that has a positive impact on EU member states and maximizes the implementation of its Cyber Security strategy.

There are several studies that have previously discussed cyber diplomacy and its relation to improving European Union cyber security. A journal written by Lucie Kadlecová and several of her colleagues entitled Cyber Security: Mapping the Role of Science Diplomacy in the Cyber Field in 2020. The journal emphasizes that the topic of cybersecurity has become part of national defense discourse for the last thirty years or so. With an increasing number of cyberattacks originating in one country and targeting another, cybersecurity is slowly getting on the agenda of the international community. According to them, The discussion on cybersecurity was initially very much related to technology and technical solutions, but as the topic has received greater attention, is now being handled by the world of international diplomacy (Kadlecová et al., 2020).

Besides that, another journal is "Cyber-diplomacy: the making of an international society in the digital age", written by André Barrinha and Thomas Renard in 2017. Barrinha & Renard describe the condition of cyberspace which according to them has become the main locus and focus International Relations. Most of the global powers have now streamlined the problems in cyberspace into their foreign policies, adopting cyber strategies and appointing appointed diplomats for strategic purposes in discussing cyber issues (Barrinha & Renard, 2017). Barrinha & Renard also concluded that the activities of the State in Cyberspace/cyberspace are still largely determined by strategic (not normative) considerations, especially in the realm (of the international system), and they also argue that cyber diplomacy aims to progressively shift these behaviors and attitudes towards peaceful cooperation. And its existence, and its existence, is determined by clear rules and principles: from interactive unit systems to state societies. In that case, cyber diplomacy for cyberspace is the same as diplomacy for International Relations which is a fundamental pillar of the international community (Barrinha & Renard, 2017).

The last journal, namely a journal written by Kasper, Osula, & Olnár entitled EU Cybersecurity and Cyber Diplomacy The year 2021. They map out existing and proposed instruments to shape the various tools/means in this broad context to get the first ideas about what we can call EU cyber diplomacy. The mapping exercise reveals that EU cyber diplomacy is a distinct set of tools that reflect the EU's need to secure its policy objectives. In chapters

1 and 2 of this journal they lay the groundwork for the global concept of cyber diplomacy and EU cybersecurity policy. In the following chapters (3 and 4) they draw attention to the apparent development of 'cyber diplomacy' in the EU (Kasper et al., 2021)

The difference between these journals and this research lies in the focus of discussion and research. Their journals focus more on discussing cybersecurity and cyber diplomacy in general and the European Union in particular by briefly explaining the methods used to strengthen cybersecurity, and can categorize into cyber diplomacy. Meanwhile, this research focuses more on the European Union's cybersecurity strategy and its implementation of the Cyber Diplomacy Toolbox (CDT) policy.

This research will explore the European Union's cyber security strategy, especially in the establishment of the CDT as one of its instruments in responding to dangerous cyber activity. It also examines more deeply how CDT has a positive impact on European Union member countries and maximizes the implementation of its Cyber Security strategy. Because the implementation of CDT in July 2020, namely in the form of imposing sanctions on freezing assets and banning travel to six individuals and three entities, was the first European Union sanction issued related to cyber issues.

The presence of CDT also still has a number of unanswered questions, especially about how CDT works and the extent of involvement of member countries in the realm of diplomacy and what tools are in it. And whether this CDT will be effective in resolving the European Union's cyber problems. Everything will be explained in this research so that in the future this study can be useful to increase readers' knowledge regarding European Union cyber issues and how to implement their cybersecurity strategy.

RESEARCH METHOD

In this study, the authors used a qualitative method to answer the research questions presented in this study. The qualitative method is a process of research and understanding based on social phenomena and problems faced by humans (Creswell, John W, 1998). The type of research that researchers use is descriptive-analytic type, which is a research activity in international relations by looking at existing problems through data collection, then analyzing by linking the data with theories in international relations (Mas'oed, M, 1994)

The results of the description will then be analyzed so that it will lead to analytic conclusions. This method is used in this study to describe and analyze the European Union's Cyber Security strategy, especially through the implementation of the Joint Cyber Diplomacy Toolbox (CBT) framework. In this research used thematic analysis techniques. This technique is also a systematic approach that involves themes or patterns contained in qualitative data.

Based on the discussion that has been determined, this study uses primary and secondary data sources. First, primary data sources can be interpreted as data obtained directly by researchers without any editing process or can be referred to as raw data. Primary data is obtained directly from the first authority without going through intermediariesObtaining data directly from the official European Union website and interviewing relevant stakeholders, in this case the researcher interviewed Katarzyna Czop, a Cyber Security Policy Advisor at The European External Action Service (EEAS), an institution that initiated the Cyber Diplomacy Toolbox (CDT) framework..

Secondly, secondary data sources are research data sources obtained by a researcher indirectly, for example secondary data sources such as through intermediary media such as books, journals, newspapers, and supporting sites related to the problem under study (Sugiono, 2008). The data obtained from various literature and the official website of the European Union is then linked to the existing problems using the theory of International Security and the Concept of Cyber Diplomacy. International Security Theory is used to analyze potential cybersecurity threats and explain efforts to prevent and overcome cyber attack activities against European Union Member States and the Concept of Cyber Diplomacy to analyze the diplomatic process in strengthening the European Union's Cyber Security strategy.

RESULT AND DISCUSSION

Cyber Attack Activities Against European Union (EU) Member Countries

The European Union's gradual involvement in cybersecurity issues was shaped by several cyber incidents, which were an unprecedented challenge and had a significant impact on the way EU member states viewed the cyber domain. The first cyber incident or cybercrime activity occurred in a European Union member state namely Estonia in 2007, attacks occurred on the president, parliament, ministries of political parties, media channels, banks and Estonian communication infrastructure. They are victims of ongoing cyberattacks believed to have been launched or carried out by Russia(Giantas, 2019).

These issues have led to the creation of a comprehensive legal, policy and institutional framework covering all major EU policy areas, including cybercrime and cyber security (Christou, 2018). The attack on Estonia's IT infrastructure was named the world's first cyber attack. This attack was the first known example of an entire country being attacked through a large-scale cyber attack. This attack is also considered to be the first time a sustained and politically motivated electronic attack has been launched to wreak havoc on a country's entire digital infrastructure (Giantas, 2019).

The cyber crime that occurred in Estonia is the beginning of a new challenge for the European Union and the World which requires the European Union to increase and maintain cooperation between the EU and other countries, especially in the field of cyber (Bendiek & Kettemann, 2021), Cooperation at the Regional and International level is needed to effectively prepare for and respond to cyberattacks (Falessi, et al., 2012). Because after the attack, the European Union also received cyberattacks on its member countries several times Cyberattacks can be carried out by individuals, but also by states for industrial espionage, for economic damage to apply pressure, or to inflict actual damage to infrastructure as an act of war (Cremer,et al.,2019).

Such as the Operation Cloud Hopper Attack", then there were also attempted attacks on the Organization for the Prohibition of Chemical Weapons (OPCW) and cyberattacks on the German Federal Parliament (Deutscher Bundestag). The first Operation Cloud Hopper attacks, this is a series of cyber-attacks with significant effect originating outside the European Union and posing external threats to the European Union or its Member States and cyber-attacks with significant effect against third countries. "Operation Cloud Hopper" targeted the information systems of multinational companies on six continents, including companies located in the European Union, and obtained unauthorized access to commercially sensitive data, resulting in significant economic losses. Actor publicly known as "APT10" ("Advanced Persistent Threats 10") (aka "Red Apollo", "CVNX", "Stone Panda", "MenuPass" and "Potassium") performs "Operation Cloud Hopper". According to the European Union, this attack was supported by Haitai Technology Development, which is a Chinese company (Official Journal of the European Union L 246, 2012).

Second, there was an attempted attack on the OPCW in the Netherlands. According to the European Union, this attack was carried out by Russian military intelligence trying to gain unauthorized access to the Wi-Fi network of the OPCW in The Hague, Netherlands, in April 2018. The attempted cyber attack was aimed at hacking the Wi-Fi network. Fi OPCW, which if successful, would jeopardize network security and OPCW's ongoing investigative work. The Netherlands Defense Intelligence and Security Service (DISS) (Militaire Inlichtingen-en Veiligheidsdienst – MIVD) thwarted an attempted cyberattack, thereby preventing serious damage to the OPCW(Official Journal of the European Union L 246, 2012). The Russian military intelligence unit, referred to as the Special Technology Center, is also said to be behind the NotPetya attack and was accused of targeting Ukraine's power grid in 2015 and 2016.

The third example is a cyber attack on the German Federal Parliament (Deutscher Bundestag). The European Union also blamed Russian intelligence as the actor behind the cyber attack on the German federal parliament (Deutscher Bundestag) in April and May 2015. This cyber attack targeted the parliament's information system and affected its operations for several days. Huge amounts of data were stolen and the email accounts of several MPs and Chancellor Angela Merkel were affected(Official Journal of the European Union L 351 I, 2020).

Such cybercrime incidents or activities demonstrate that cyber conflicts are becoming commonplace around the world, including Europe and highlight the emerging need for national security strategies and policies to competently factor cyber threats and conflicts into all stages of security planning. Human conflict is no longer just attached to the physical world. It's also happening in the new domain of cyberspace. Cyberthreats often go undetected for a long time, become increasingly sophisticated, can have a major impact on the economy and society, modern lifestyles and national security (Giantas, 2019). Despite the emergence of cyber threats, the European Union, which initially did not have the necessary policies and frameworks to deal with them at the collective level of the European Union, then began to develop its cybersecurity strategy and one of the results was the birth of the Cyber Diplomacy Toolbox (CDT) as a Joint Diplomatic Response to the European Union. Against Threats of cyber attack activity.

European Union Efforts to Respond the Threat of Cyber Attack Activities Using the Cyber Diplomacy Toolbox (CDT)

One part of the European Union's cybersecurity strategy in the digital era, namely the field of Building Operational Capacity to Prevent, Deter and Respond (Building Operational Capacity to Prevent, Obstruct and Respond) in this field one of the steps/actions used is the use of The Cyber Diplomacy Toolbox by (CDT) EU. In practice, the EU has used a cyber diplomacy toolbox to prevent, deter, deter and respond to malicious cyber activity. Malicious cyber activities, should be addressed by an effective and comprehensive joint EU diplomatic response, using the various measures available at EU level (European Commission - Cyber Strategy, 2020).

Fast and effective CDT requires solid shared situational awareness and the ability to quickly prepare for a common EU position. The High Representative of the Union for Foreign Affairs and Security Policy will encourage and facilitate the creation of a European Union Member State cyber intelligence working group within the EU Intelligence and Situation Center (INTCEN), to advance strategic intelligence cooperation on cyber threats and activity. This will further support EU situational awareness and decision making on Joint diplomatic response or CDT (European Commission - Cyber Strategy, 2020).

The conceptual framework for CDT as part of the EU's approach to cyber diplomacy has several functions, namely:

1. Contribute to conflict prevention, mitigation of cybersecurity threats, and greater stability in international relations.
2. Contribute to strengthening the rules-based international order in cyberspace including the application of international law and adherence to norms of responsible state behavior.
3. Encourage cooperation, facilitate threat mitigation and influence behavior in the long term.

4. Allows the EU and its Member States to take advantage of their diplomatic instruments, including restrictive measures, to keep cyberspace global, open, stable and secure. (Czop, Katarzyna Online Interview, May 19 2022).

Further discussion of CDT in the EU cyber security strategy is based on several institutional frameworks, namely Council Conclusions (June 2017), Implementing Guidelines (October 2017), Adoption of a horizontal cyber sanctions regime (May 2019) and Guidelines on coordinated attribution at EU level (June 2019). The Framework has a mechanism to Collaborate to collect and assess situational awareness, any response actions are part of the Common Foreign and Security Policy, has strategic public communication procedures, and practices to cooperate and coordinate with international partners tothis framework (Czop, Katarzyna Online Interview, May 19 2022).

In seeing the urgency of the Cooperation through CDT framework, the European Union considers that a common and comprehensive approach to cyber diplomacy can contribute to conflict prevention, mitigation of cybersecurity threats, and greater stability in international relations. The EU and its Member States note the importance of the ongoing EU cyber diplomacy engagement and the need for coherence among EU cyber initiatives to effectively strengthen cyber resilience, and are encouraged to further intensify their efforts on cyber dialogue within an effective framework. policy coordination, and emphasized the importance of cyber capacity in building cooperation with third countries(Council of the European Union, 2017b).

The Cyber Diplomacy Toolbox(CDT) As the European Union's Joint Diplomatic Response to Threats of attack activity or cybercrime is an important part of the EU in enhancing its Cyber Security Strategy. The European Union confirms that for Optimization of the framework for CDT Cooperation Implementation will use measures in the Common Foreign and Security Policy, Including, where necessary, restrictive measures, adopted under the relevant provisions of the Treaty, suitable for the Framework for a joint EU diplomatic response to harmful cyber activity and should promote cooperation, facilitate the mitigation of immediate and long-term threats, and influence the long-term behavior of potential aggressors.(Council of the European Union, 2017).

In cases where malicious cyber activity is being carried out by a State, as well as in cases where a State is held responsible for the actions of a non-state actor acting under its direction or control, or if this State recognizes and adopts the behavior of a non-state actor as part of its from it, various measures in the CDT, including restrictive measures against that State, may be used by the EU and its Member States.When it comes to potential collective responses, it is important that they too are bound by and comply with international law. On the other hand, self-defense is also a legitimate response(Kiviuht, 2020).

In the case of a State that knowingly allows its territory to be used for malicious cyber activity, including actions deemed wrong by international law using ICTs, against a Member State or the EU, the steps in this CDT can also be used to encourage that State to ensure that the territory is not used for such activities. This provision is contained in the Directive on Attacks against Information Systems (2013/40/EU). In further implementation, CDT has at least five action steps, namely Preventive measures, Cooperative measures, Stabilizing measures, Restrictive measures and Supportive measures. Actions may be public or private, and may also be accompanied by coordinated attribution at the EU level*(Council of the European Union*- CDT Guidelines, 2017).

These measures may be used either independently, sequentially or in parallel as part of a coherent strategic approach at EU level designed and implemented to influence specific actors, and should take into account the broader context of EU external relations and the broader EU approach that aims to contribute to cyber threat mitigation, conflict prevention and greater stability in international relations.

On 7 June 2017, the EU officially adoptedframework for Joint Diplomatic Response to Cyber-attack threats known as the Cyber Diplomacy Toolbox (CDT). This is contained in the Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox") – Adoption which was published directly by the European Council in decision number 9916/17(Council of the European Union, 2017). In its conclusion the European Council as the representative of the EU recognized that cyberspace offers significant opportunities, but also presents growing challenges for EU external policies, including for the Common Foreign and Security Policy or CFSP, and emphasized the growing need to protect EU integrity and security for EU member states, and their citizens against cyber threats and malicious cyber activity.

In seeing the urgency of the Cooperation through CDT framework, the European Union considers that a common and comprehensive approach to cyber diplomacy can contribute to conflict prevention, mitigation of cybersecurity threats, and greater stability in international relations. The EU and its Member States note the importance of the ongoing EU cyber diplomacy engagement and the need for coherence among EU cyber initiatives to effectively strengthen cyber resilience, and are encouraged to further intensify their efforts on cyber dialogue within an effective framework. policy coordination, and emphasized the importance of cyber capacity in building cooperation with third countries(Council of the European Union, 2017).

The Cyber Diplomacy Toolbox(CDT) As a Joint European Union Diplomatic Response to Threats of cybercrime or attack activity is an important instrument for the EU in enhancing its Cyber Security Strategy as well as building capacity in law enforcement and judiciary, working with industry, and enhancing capabilities to deal with cyberattacks (Renard, 2014). The European Union confirms that for Optimization of the framework for CDT

Cooperation Implementation will use measures in the Common Foreign and Security Policy, Including, where necessary, restrictive measures, adopted under the relevant provisions of the Treaty, suitable for the Framework for joint EU diplomatic response to harmful cyber activity and should encourage cooperation, facilitating the mitigation of immediate and long-term threats, and influencing the long-term behavior of potential aggressors. The EU will work on the further development of the Framework for a joint EU diplomatic response to malicious cyber activity (Council of the European Union, 2017).

The author found that since the initial adoption of this Cooperation, CDT Implementation through the Joint Foreign and Security Policy has been used on two occasions with Since the framework came into effect, it has been used on two occasions by imposing sanctions. Sanctions are one of the options available within the Union's framework for joint diplomatic response to malicious cyber activity (the so-called cyber diplomacy toolbox or CDT) and are intended to prevent, deter, and respond to continued and escalating malicious behavior in cyberspace. The European Union Council imposes sanctions in the form of travel bans and asset freezes imposed on individuals, and asset freezes imposed on institutions or institutions. In addition, EU persons and entities are prohibited from making funds available to those listed. Sanctions which are the implementation of this CDT were first imposed or given on July 30, 2020 to Russian, Chinese and North Korean hackers who were involved in various cyber attacks such as the so-called “Wannacry” and “NotPetya” attacks. Furthermore, On October 22, 2020, a second sanction was imposed against Russian hackers for participating in the cyberattack that hit the German Parliament in 2015.

On 30 July 2020, for the first time, the European Union imposed an asset freeze and travel ban on six individuals and three entities responsible for or involved in multiple cyber attacks including attempted attacks on the Organization for the Prohibition of Chemical Weapons (OPCW) which publicly known as “WannaCry”, “NotPetya” and “Operation Cloud Hopper”(Francesco Guarascio, 2020). These sanctions are the first sanctions issued by the European Union regarding cyber threats or CyberCrime Actions against its member countries. These are contained in the Declaration of the EU High Representative for Foreign Affairs and Security Policy Josep Borrell on the European Union's response to promoting international defense security and stability in cyberspace in Council Decision (CFSP) 2020/1127 (2020) L 246/12 and Council Implementing Regulation (EU) 2020/1125 L 246/4 on Restrictive measures against cyber attacks that threaten the Union or its Member countries(Official Journal of the European Union L 246, 2012)

Then, on 22 October 2020, the European Union for the second time re-imposed sanctions in the form of a travel ban and asset freeze on two individuals and one agency responsible for or taking part in cyber attacks against the German Federal Parliament (Deutscher Bundestag) in April and May 2015. This cyber attack targeted the parliamentary information system and affected its ability to operate for several days. Huge amounts of data were stolen and the email accounts of several MPs, including Chancellor Angela Merkel, were affected. The relevant legal actions, including the names of the persons and bodies concerned, have been published in the Official Journal of the European Union which discusses aboutCouncil Implementing Regulation (EU) 2020/1536 & Council Decision (CFSP) 2020/1537. With this decision, it means that the European Union has applied sanctions to a total of 8 people and 4 entities (Table.1) and bodies in connection with cyber attacks targeting the EU or its member countries(The Council of the European Union, 2020).

Granting of European Union Cyber Sanctions through Cyber Diplomacy Toolbox (CDT)

The imposition of sanctions related to Cybercrime is a form of the European Union's seriousness in improving its Cybersecurity Strategy. That the European Union will focus on increasing its defense and security from cyber threats against its Member countries, among others, through the CBT supported by the CFSP. In the Treaty of the European Union (TEU), it is stated that the European Union is also aimed at resolving matters related to the implementation of the Common Foreign and Security Policy (CFSP) including a progressive framework of the Joint defense and security policy which leads to joint defense in accordance with the provisions of Article 42 TEU, thereby strengthening its European identity and independence to promote peace, security and progress in Europe and in the world (Official Journal of the European Union (C326, 2012). Related to this,

Regarding the official decision, published by the European Union, For the first sanctions listed in Council Decision (CFSP) 2020/1127 (2020) L 246/12 and Council Implementing Regulation (EU) 2020/1125 L 246/4 and for sanctions both are listed in Council Implementing Regulation (EU) 2020/1536 & Council Decision (CFSP) 2020/1537. The researcher has also summarized and processed it into data (Table.1) which contains complete data regarding Name (Individual/Institution), Information that can be identified, Reasons for being sanctioned and Date entered into the list or date of commencement of sanctions.

The entire List List (Table.1), namely for eight individuals and four entities, is given a sanction of freezing assets and a travel ban. It started since its decision was issued, namely some started from 30 July 2020 and some started from 22 October 2020. However, On 17 May 2021, the Council again decided to extend the framework for restrictive measures against cyber-attacks that threaten the EU or its member states for one another year, until May 18, 2022 . And finally, on May 16, 2022, the Foreign Affairs Council again extended sanctions against cyber attacks that threaten the EU and its member states until May 18, 2025. That means that all those on the list are still subject to sanctions. (The Council of the European Union, 2021).

In implementing the CDT, the European Union establishes a framework for sanctions against cyberattacks that threaten the EU or its member states based on two Instruments namely Council Decision (CFSP) 2019/797 and Council Regulation (EU) 2019/796. The imposition of these sanctions is included in the Restrictive measures section in the stages of implementing CDT, the imposition of these sanctions applies to cyber attacks and cyber attack attempts with the following criteria:

1. Has a significant effect;
2. Which is an external threat to the European Union or its Member States;
3. Involving or entering: Access to information systems, information system disturbances, data disturbances, wiretapping of data, and matters beyond their authority (Czop, Katarzyna Online Interview, May 19 2022).

All dangerous cyber attack activities which include cyber attacks and will be given targeted actions in the form of sanctions such as travel bans and asset freezing and will be included in list of natural and legal persons, entities and bodiess deemed responsible for cyber attacks, which providing financial, technical or material support, Who is involved in the cyber attack and in relation to the other persons listed (Czop, Katarzyna Online Interview, May 19 2022).

Table 1. List of natural persons out to Regulation (EU) 2019/796. Decision Attachment (CFSP).

No	name	Identifying information	reasons	Date of listing
1.	GAO Qiang	Place of birth: Shandong Province, China Address: Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin, China Nationality: Chinese	Gao Qiang is involved in “Operation Cloud Hopper”, a series of cyber-attacks with a significant effect originating from outside the Union and constituting an external threat to the Union or its Member States and of cyber-attacks with a significant effect against third States . “Operation Cloud Hopper” targeted information systems of multinational companies in six continents, including companies located in the Union, and gained unauthorized access to commercially	30.7.2020

		Gender: male	sensitive data, resulting in significant economic loss. The actor publicly known as “APT10” (“Advanced Persistent Threat 10”) (aka “Red Apollo”, “CVNX”, “Stone Panda”, “MenuPass” and “Potassium”) carried out “Operation Cloud Hopper”. Gao Qiang can be linked to APT10, including through his association with APT10 command and control infrastructure. Moreover, Huaying Haitai, an entity designated for providing support to and facilitating “Operation Cloud Hopper”, employed Gao Qiang. He has links with Zhang Shilong, who is also designated in connection with "Operation Cloud Hopper". Gao Qiang is therefore associated with both Huaying Haitai and Zhang Shilong.	
2.	Zhang Shilong	Address: Hedong, Yuyang Road No. 121, Tianjin, China Nationality: Chinese Gender: male	Zhang Shilong is involved in “Operation Cloud Hopper”, a series of cyber-attacks with a significant effect originating from outside the Union and constituting an external threat to the Union or its Member States and of cyber-attacks with a significant effect against third States . “Operation Cloud Hopper” has targeted information systems of multinational companies in six continents, including companies located in the Union, and gained unauthorized access to commercially sensitive data, resulting in significant economic loss. The actor publicly known as “APT10” (“Advanced Persistent Threat 10”) (aka “Red Apollo”, “CVNX”, “Stone Panda”, “MenuPass” and “Potassium”) carried out “Operation Cloud Hopper”. Zhang Shilong can be linked to APT10, including through the malware he developed and tested in connection with the cyber-attacks carried out by APT10. Moreover, Huaying Haitai, an entity designated for providing support to and facilitating “Operation Cloud Hopper”, employed Zhang Shilong. He has links with Gao Qiang, who is also designated in connection with "Operation Cloud Hopper". Zhang Shilong is therefore associated with both Huaying Haitai and Gao Qiang.	30.7.2020
3.	Alexey Valeryevich MININ	Алексей Валерьевич МИНИН	Alexey Minin took part in an attempted cyber-attack with a potentially significant effect against the Organization for the	30.7.2020

		Date of birth: May 27, 1972 Place of birth: Perm Oblast, Russian SFSR (now Russian Federation) Passport number: 120017582 Issued by: Ministry of Foreign Affairs of the Russian Federation Validity: from 17 April 2017 to 17 April 2022 Location: Moscow, Russian Federation Nationality: Russian Gender: male	Prohibition of Chemical Weapons (OPCW) in the Netherlands. As a human intelligence support officer of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU), Alexey Minin was part of a team of four Russian military intelligence officers who attempted to gain unauthorized access to the Wi -Fi network of the OPCW in The Hague, the Netherlands, in April 2018. The attempted cyber-attack was aimed at hacking into the Wi-Fi network of the OPCW, which, if successful, would have compromised the security of the network and the OPCW's ongoing investigative work. The Netherlands Defense Intelligence and Security Service (DISS) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) disrupted the attempted cyber-attack, thereby preventing serious damage to the OPCW.	
4.	Alexei Sergeyvich MORENETS	Алексей Сергеевич МОРЕНЕЦ Date of birth: July 31, 1977 Place of birth: Murmanskaya Oblast, Russian SFSR (now Russian Federation) Passport number: 100135556 Issued by: Ministry of Foreign Affairs of the Russian Federation Validity: from 17 April 2017 to 17 April 2022	Aleksei Morenets took part in an attempted cyber-attack with a potentially significant effect against the Organization for the Prohibition of Chemical Weapons (OPCW) in the Netherlands. As a cyber-operator for the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU), Aleksei Morenets was part of a team of four Russian military intelligence officers who attempted to gain unauthorized access to the Wi-Fi Fi network of the OPCW in The Hague, the Netherlands, in April 2018. The attempted cyber-attack was aimed at hacking into the Wi-Fi network of the OPCW, which, if successful, would have compromised the security of the network and the OPCW's ongoing investigative work. The Netherlands Defense Intelligence and Security Service (DISS) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) disrupted the attempted cyber-attack, thereby preventing serious damage to the OPCW.	30.7.2020

		Location: Moscow, Russian Federation Nationality: Russian Gender: male		
5.	Evgenii Mikhaylovich SEREBRIAKOV	Евгений Михайлович СЕРЕБРЯКОВ Date of birth: 26 July 1981 Place of birth: Kursk, Russian SFSR (now Russian Federation) Passport number: 100135555 Issued by: Ministry of Foreign Affairs of the Russian Federation Validity: from 17 April 2017 to 17 April 2022 Location: Moscow, Russian Federation Nationality: Russian Gender: male	Evgenii Serebriakov took part in an attempted cyber-attack with a potentially significant effect against the Organization for the Prohibition of Chemical Weapons (OPCW) in the Netherlands. As a cyber-operator for the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU), Evgenii Serebriakov was part of a team of four Russian military intelligence officers who attempted to gain unauthorized access to the Wi-Fi network of the OPCW in The Hague, the Netherlands, in April 2018. The attempted cyber-attack was aimed at hacking into the Wi-Fi network of the OPCW, which, if successful, would have compromised the security of the network and the OPCW's ongoing investigative work. The Netherlands Defense Intelligence and Security Service (DISS) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) disrupted the attempted cyber-attack, thereby preventing serious damage to the OPCW.	30.7.2020
6.	Oleg Mikhaylovich SOTNIKOV	Олег Михайлович СОТНИКОВ Date of birth: 24 August 1972 Place of birth: Ulyanovsk, Russian SFSR (now Russian Federation) Passport	Oleg Sotnikov took part in an attempted cyber-attack with a potentially significant effect against the Organization for the Prohibition of Chemical Weapons (OPCW), in the Netherlands. As a human intelligence support officer of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU), Oleg Sotnikov was part of a team of four Russian military intelligence officers who attempted to gain unauthorized access to the Wi -Fi network of the OPCW in The	30.7.2020

		number: 120018866 Issued by: Ministry of Foreign Affairs of the Russian Federation Validity: from 17 April 2017 to 17 April 2022 Location: Moscow, Russian Federation Nationality: Russian Gender: male	Hague, the Netherlands, in April 2018. The attempted cyber-attack was aimed at hacking into the Wi-Fi network of the OPCW, which, if successful, would have compromised the security of the network and the OPCW's ongoing investigative work. The Netherlands Defense Intelligence and Security Service (DISS) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) disrupted the attempted cyber-attack, thereby preventing serious damage to the OPCW.	
7.	Dmitry Sergeyevich BADIN	Дмитрий Сергеевич БАДИН Date of birth: November 15, 1990 Place of birth: Kursk, Russian SFSR (now Russian Federation) Nationality: Russian Gender: male	Dmitry Badin took part in a cyber-attack with a significant effect against the German federal parliament (Deutscher Bundestag). As a military intelligence officer of the 85th Main Center for Special Services (GTsSS) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU), Dmitry Badin was part of a team of Russian military intelligence officers which conducted a cyber-attack against the German federal parliament (Deutscher Bundestag) in April and May 2015. This cyber-attack targeted the parliament's information system and affected its operation for several days. A significant amount of data was stolen and the email accounts of several MPs as well as of Chancellor Angela Merkel were affected.	22.10.2020

8.	Igor Olegovich KOSTYUKOV	Игорь Олегович КОСТЮКОВ Date of birth: 21 February 1961 Nationality: Russian Gender: male	Igor Kostyukov is the current Head of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU), where he previously served as First Deputy Head. One of the units under his command is the 85th Main Center for Special Services (GTsSS), also known as “military unit 26165” (industry nicknames: “APT28”, “Fancy Bear”, “Sofacy Group”, “Pawn Storm” and “Strontium”). In this capacity, Igor Kostyukov is responsible for cyber-attacks carried out by the GTsSS, including those with a significant effect constituting an external threat to the Union or its Member States. In particular, military intelligence officers of the GTsSS took part in the cyber-attack against the German federal parliament (Deutscher Bundestag) which took place in April and May 2015 and the attempted cyber-attack aimed at hacking into the Wi-Fi network of the Organization for the Prohibition of Chemical Weapons (OPCW) in the Netherlands in April 2018. The cyber-attack against the German federal parliament targeted the parliament's information system and affected its operation for several days. A significant amount of data was stolen and email accounts of several MPs as well as of Chancellor Angela Merkel were affected.	22.10.2020

Table 2. List legal persons, entities and bodiess set out to Regulation (EU) 2019/796. Decision Attachment (CFSP).

No	name	Identifying information	reasons	Date of listing
1	Tianjin Huaying Haitai Science and Technology Development Co. Ltd (Huaying Haitai)	aka: Haitai Technology Development Co. Ltd Location: Tianjin, China	Huaying Haitai provided financial, technical or material support for and facilitated “Operation Cloud Hopper”, a series of cyber-attacks with a significant effect originating from outside the Union and constituting an external threat to the Union or its Member States and of cyber-attacks with a significant effect against third States. “Operation Cloud Hopper” has targeted information systems of	30.7.2020

			multinational companies in six continents, including companies located in the Union, and gained unauthorized access to commercially sensitive data, resulting in significant economic loss. The actor publicly known as “APT10” (“Advanced Persistent Threat 10”) (aka “Red Apollo”, “CVNX”, “Stone Panda”, “MenuPass” and “Potassium”) carried out “Operation Cloud Hopper”. Huaying Haitai can be linked to APT10. Moreover, Huaying Haitai employs Gao Qiang and Zhang Shilong, who are both designated in connection with "Operation Cloud Hopper". Huaying Haitai is therefore associated with Gao Qiang and Zhang Shilong.	
2.	Chosun Expo	aka: Chosen Expo; Korea Export Joint Venture Location: DPRK	Chosun Expo provided financial, technical or material support for and facilitated a series of cyber-attacks with a significant effect originating from outside the Union and constituting an external threat to the Union or its Member States and of cyberattacks with a significant effect against third States, including the cyber-attacks publicly known as “WannaCry” and cyber-attacks against 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. “WannaCry” disrupted information systems around the world by targeting information systems with ransomware and blocking access to data. It affected information systems of companies in the Union, including information systems relating to services necessary for the maintenance of essential services and economic activities within Member States. The actor publicly known as “APT38” (“Advanced Persistent	30.7.2020

			Threat 38”) or the “Lazarus Group” carried out “WannaCry”. Chosun Expo can be linked to APT38/the Lazarus Group, including through the accounts used for the cyber-attacks.	
3.	Main Center for Special Technologies (GTsST) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU)	Address : 22 Kirova Street, Moscow, Russian Federation	The Main Center for Special Technologies (GTsST) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU), also known by its field post number 74455, is responsible for cyber-attacks with a significant effect originating from outside the Union and constituting an external threat to the Union or its Member States and for cyber-attacks with a significant effect against third States, including the cyber-attacks publicly known as “NotPetya” or “EternalPetya” in June 2017 and the cyber-attacks directed at an Ukrainian power grid in the winter of 2015 and 2016. 30.7.2020' EN Official Journal of the European Union 30.7.2020 L 246/17 “NotPetya” or “EternalPetya” rendered data inaccessible in a number of companies in the Union, wider Europe and worldwide, by targeting computers with ransomware and blocking access to data, resulting among others in significant economic loss. The cyberattack on a Ukrainian power grid resulted in parts of it being switched off during winter. The actor publicly known as “Sandworm” (aka “Sandworm Team”, “BlackEnergy Group”, “Voodoo Bear”, “Quedagh”, “Olympic Destroyer” and “Telebots”), which is also behind the attack on the Ukrainian power grid , carried out “NotPetya” or “EternalPetya”. The Main Center for Special Technologies of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation has an active role in the cyber-activities undertaken by	30.7.2020'

			Sandworm and can be linked to Sandworm.	
4	85th Main Center for Special Services (GTsSS) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU)	Address: Komsomol'skiy Prospect, 20, Moscow, 119146, Russian Federation	The 85th Main Center for Special Services (GTsSS) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU), also known as “military unit 26165” (industry nicknames: “APT28”, “Fancy Bear”, “Sofacy Group”, “Pawn Storm” and “Strontium”), is responsible for cyber-attacks with a significant effect constituting an external threat to the Union or its Member States. In particular, military intelligence officers of the GTsSS took part in the cyber-attack against the German federal parliament (Deutscher Bundestag) which took place in April and May 2015 and the attempted cyber-attack aimed at hacking into the Wi-Fi network of the Organization for the Prohibition of Chemical Weapons (OPCW) in the Netherlands in April 2018. The cyber-attack against the German federal parliament targeted the parliament's information system and affected its operation for several days. A significant amount of data was stolen and.	22.10.2020'

Entire List List (Table.1 and table 2) loada list of names of perpetrators, Identified Information and reasons for imposing sanctions against the entity, as well as the date of determination. The list has been given to the government of the country concerned as well as giving a warning that the European Union now has strict sanctions against perpetrators of cyber attacks, especially against its member countries.

CONCLUSION

Cyber Diplomacy Toolbox(CDT) is the European Union's ambitious attempt to create a legal order in cyberspace using the sanctions model through the CFSP in response to cyberattacks. Since the CDT in EU Adoption and this framework entered into force, its application has been made on two occasions. In July 2020, the Council of the European Union imposed sanctions on Russian, Chinese and North Korean hackers involved in various cyber attacks such as the so-called "Wannacry" and "NotPetya" attacks. And in October 2020, a new set of sanctions was imposed against Russian hackers for participating in the cyberattacks that hit the German Parliament in 2015. Overall these sanctions policies were weighted on eight individuals and four entities judged to have committed crimes and cyberattacks against EU Member States.

The researchers found that the European Union's reason for adopting CDT was that the European Union wanted to build trust between Member States in carrying out cyber cooperation to strengthen cyber security with the European Union. The fact that the European Union did not address cyber issues at all at the time of its formation makes cyber issues a new challenge to the development of the European Union and the cyber security of its Member states. Another reason the European Union adopted CDT is also because the European Union does not yet have a specific tool to crack down on cyber actors. The European Union already has specific regulations and institutions that focus on cyber issues, and CDT is intended as a tool for the European Union to take action against cyber actors.

BIBLIOGRAPHY

Barrinha, A., & Renard, T. (2017). Cyber-diplomacy: the making of an international society in the digital age. Global Affairs, 3(4–5), 353–364. https://doi.org/10.1080/23340460.2017.1414924

Bendiek, A. (2014). Tests of Partnership : Transatlantic Cooperation in Cyber Security, Internet Governance, and Data Protection. SWP Research Paper, March.

Cardwell, PJ (2015). The legalization of european union foreign policy and the use of sanctions. Cambridge Yearbook of European Legal Studies, 17(May), 287–310. https://doi.org/10.1017/cel.2015.11

Christou, G. (2018). The collective securitization of cyberspace in the European Union European Union. West European Politics, 0(0), 24. https://doi.org/10.1080/01402382.2018.1510195

Council of the European Union. (2017). CDT Guideline - Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities - approval of the final tex. October.

Council of the European Union. (2017). Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (“Cyber Diplomacy Toolbox”). Official Journal of the European Union, 9916(17), 1–5.

Czop, Katarzyna,(2022), Online Interview, "The Cyber Diplomacy Toolbox by EEAS" May, 19 2022.

European External Action Service (EEAS). (2019). Common Foreign and Security Policy (CFSP). European External Action Service (EEAS). https://eeas.europa.eu/topics/common-foreign-security-policy-cfsp/420/common-foreign-and-security-policy-cfsp_en

Fahmi, C. (2008). the Eu and Peace Building in Aceh-Indonesia : 63–73.

Falessi, Nicole. Gavrila, Razvan. Klejnstrup, Maj Ritter. Moulinos, K. (2012). National Cyber Security Strategies (Practical Guide on Development and Execution). The European Network and Information Security Agency (ENISA), December.

Francesco Guarascio. (2020). EU sanctions Russian intelligence, North Korean, Chinese firms over alleged cyberattacks. Www.Reuters.Com. https://www.reuters.com/article/us-eu-cybercrime-russia-sanctions-idUSKCN24V32Q

Giantas, DH (2019). Cybersecurity in the EU: Threats, Frameworks and Future Perspectives. Laboratory of Intelligence & Cyber-Security, September, 39.

Hadith, TR (2020). Legal Protection for Certain Time Workers Based on Law Number 13 of 2003 concerning Manpower. Journal of Ideas, 6 Number 2(May), 203–212. https://doi.org/10.32884/ideas.v%vi%i.267

Hamonangan, I. (2020). Cyber Diplomacy : Towards a Peaceful International Society in. Padjadjaran Journal of International Relations (PADJIR), 1(4), 342–363. https://doi.org/10.24198/padjir.v1i4.26246

Howworth, J., & Menon, A. (2005). The european union and national defense policy. In The European Union and National Defense Policy. https://doi.org/10.4324/9780203982921

Kadlecová, L., Meyer, N., Cos, R., & Ravinet, P. (2020). Cyber Security: Mapping the Role of Science Diplomacy in the Cyber Field. Science Diplomacy in the Making: Case-Based Insights from the S4D4C Project, 770342, 62.

Kasper, A., Osula, A., & Molnár, A. (2021). EU cyber security and cyber diplomacy. 34(34), 1–15.

Kiviuht, J. (2020). The EU Cyber Diplomacy Toolbox. Master's Thesis Program HAJM, Specialization Law and Technology, 1–57.

Knapp, KJ (2009). Cyber security and global information assurance: Threat analysis and response solutions. In Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions. https://doi.org/10.4018/978-1-60566-326-5

Cremer, Steve. Mé, L., & Rémy, Didier & Roca, V. (2019). Cybersecurity Current challenges and Inria's research directions.

Moret, E., & Pawlak, P. (2017). The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime? July, 1–4. https://www.iss.europa.eu/content/eu-cyber-diplomacy-toolbox-towards-cyber-sanctions-regime

Official Journal of the European Union L 246. (2012). Consolidated Version of the Treaty on European Union (C326). Core EU Legislation, 55, 13–45. https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0023.02/DOC_1&format=PDF

Official Journal of the European Union L 351 I. (2020). Council Implementing Regulation (EU) 2020/1536 & Council Decision (CFSP) 2020/1537. Official Journal of the European Union L351I, 63(7 December 2020), 1–19.

Potter, EH (2002). Cyber-Diplomacy : Managing Foreign Policy in the Twenty-First Century. In McGill-Queen's University Press.

Renard, T. (2014). The rise of cyber-diplomacy: the EU, its strategic partners and cyber-security. june. http://fride.org/download/WP7_The_rise of_cyber_ diplomacy.pdf

Sliwinski, KF (2014). Moving beyond the European Union's Weakness as a Cyber-Security Agent. Contemporary Security Policy, 35(3), 468–486. https://doi.org/10.1080/13523260.2014.959261

The Council of the European Union. (2020a). EU imposes the first ever sanctions against cyber-attacks. The Council of the European Union. https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/#:~:text= These include the attempted cyber, ban and an asset freeze.

The Council of the European Union. (2020b). Malicious cyber-attacks: EU sanctions two individuals and one body over 2015 Bundestag hack. https://www.consilium.europa.eu/en/press/press-releases/2020/10/22/malicious-cyber-attacks-eu-sanctions-two-individuals-and-one-body-over-2015- bundestag-hack/

The Council of the European Union. (2021). Cybersecurity: Council adopts conclusions on the EU's cybersecurity strategy. https://www.consilium.europa.eu/en/press/press-releases/2021/03/22/cybersecurity-council-adopts-conclusions-on-the-eu-s-cybersecurity-strategy/

The Council of the European Union. (2021). Cyber-attacks: Council prolongs framework for sanctions for another year. https://www.consilium.europa.eu/en/press/press-releases/2021/05/17/cyber-attacks-council-prolongs-framework-for-sanctions-for-another-year/