TALLINN UNIVERSITY OF TECHNOLOGY

School of Business and Governance

Department of Law

Juho Kivihuhta

The EU Cyber Diplomacy Toolbox

Master's thesis

Programme HAJM,

Specialisation law and technology

Supervisor: Agnes Kasper PhD

Tallinn 2020

I declare that the I have compiled the paper independently and all works, important standpoints and data by other authors have been properly referenced and the same paper has not been previously been presented for grading. The document length is 17014 words from the introduction to the end of summary.

Juho Kivihuhta

……

(signature, date)

Student code: 184459HAJM Student e-mail address: juho.kivihuhta@live.fi

Supervisor: Agnes Kasper, PhD:

The paper conforms to requirements in force

……

(signature, date)

Chairman of the Defence Committee: /to be added only for graduation theses/

Permitted to the defence

……

(name, signature, date)

Table of contents

Abstract

Governments are increasingly using cyberspace to achieve political and strategic goals. Cyber operations are also aimed at stealing military secrets. Industrial espionage is done in order to achieve an advantage in the market. Critical infrastructure has also been targeted. Cyberspace is subject to international laws, and international laws and customary norms regulate what is legal and what is not. The increasing amount of different types of cybercrimes has lead the EU's efforts to protect EU Member States and Institutions. The cyber sanction regime was finally established by Council Decision 2019/797 and Council Regulation 2017/796. The Decision and Regulation contain the substantial elements of the EU Cyber Diplomacy Toolbox against cybercrimes. Toolbox uses sanctions to deter criminals from engaging in malicious cyber operations and single out those that aren't deterred. The sanctioning methods are travel bans and freezing of assets, which aim to bring about a more peaceful and organized cyberspace. Attributing attacks to persons or entities creates difficulty in the process and attribution creates further problems due to the fact that attributing an attacker remains the sovereign decision of the Member States. The research in this thesis look at the first application of the Toolbox on July on 30 July 2020. Experiences gained from other sanction regimes are evaluated in relation to the Toolbox and its aims to follow the rules of international law and its aims to apply methods in line with the principle of proportionality. This thesis evaluates the Toolbox's application as a deterrent and looks at the Toolbox's relationship to international law, due diligence, cryptocurrencies, co-operation with the private sector, and the aspect of attribution.

Keywords: cyberspace, attribution, due diligence, cyber diplomatic toolbox

ABBREVIATIONS

CERT Computer Emergency Response Team

CFSP Common Foreign Security Policy

COREPER Committee of Permanent Representatives

CSDP Common Security and Defense Policy

CSIRTs Computer Security Incident Response Teams

EEAS European External Action Service

EUISS European Union Institute for Security Studies

ENISA European Union Agency for Cybersecurity

GRU Main Intelligence Directorate of the General Staff of the Russian Armed Forces

ICJ International Court of Justice

ICT Information and Communication Technology

NATO North Atlantic Treaty Organization

NCSC National Cyber Security Center

NIS Network and Information Security

NSA National Security Agency

OPCW Organization for the Prohibition of Chemical Weapons

OSCE Organization for Security and Cooperation in Europe

RELEX Working Party of Foreign Relations Counsellors

TEU Treaty on European Union

TFEU Treaty on the Functioning of the European Union

UN United Nations

UNGGE United Nations Group of Governmental Experts

UNSC United Nations Security Council

WTO World Trade Organization

1. INTRODUCTION

Cyberspace, the system that provides nearly global communication possibilities, has developed into a sort of natural ecosystem, and as in nature, hostile and threatening forms of communication have become a part of it. These threats can come in many forms, with computer viruses being one of the most proficient methods of disrupting activity and engaging in criminal activities such as theft, extortion, and data or property destruction. We have seen examples of these in the forms of Wannacry, ransomware originating from Korea and all over the world, or Stuxnet, a computer worm that targeted a nuclear facility in Iran, both of which will be reviewed in detail in the second chapter of this study. These viruses not only pose staggering problems for commercial agents and legislators but also for international relations. In one of the most recent events, the president of the European Commission, Ursula von der Leyen, called out China's involvement in attacks against Czech hospitals during the coronavirus pandemic.[1] The potential of states engaging in espionage or cyber warfare against another state has never been as great as it is today. Additionally, the financial world is inextricably connected to cyberspace, which makes it more vulnerable to cybercrimes. Another grave problem in the current situation is that the capabilities of developing effective means of hostility lie not only in the hands of states but can be carried out by groups or even private individuals, as in the case of the Love Letter virus in May 2000, which sent infected emails from infected Outlook accounts using their address book.[2] Therefore there is a demand for measures that can be taken to prevent, defend against, or fix threatening situations in the cyber domain. In addition, all of the measures mentioned above need to be proportional to the threat or attack that they are aimed against. Diplomatic tools are one approach to these types of cyber scenarios, and the EU Cyber Diplomatic Toolbox (referred to as Toolbox from now on) is one of the newest ways that the EU approaches the issue.

[1] Laurens, C. (2020, June 22) Von der Leyen calls out China for hitting hospitals with cyberattacks. Politico
[2] Kaspersky Threats, EMAIL-WORM.VBS.LOVELETTER, https://threats.kaspersky.com/en/threat/Email-Worm.VBS.LoveLetter/ 16th October 2020.

In international diplomacy there are certain steps which states can take in order to deal with a hostile nation, such as placing an embargo, freezing assets of a malicious actor, demanding the state to take responsibility, to name a few. There is great concern about the ability of diplomatic cyber responses to protect markets since commerce has moved to cyberspace nearly completely. This means that a cyberattack on one EU state can affect many others. The EU having developed a single market for its Member States, it has taken on the of task trying to achieve a response mechanism that can protect the single market and act on behalf of the Member States. It is extremely important to use sanctions proportionally in the financial sector. The Toolbox is a new instrument that aims to specifically affect diplomatic responses to international situations, meaning threats or conflicts arising between the EU and a third state or states. The Toolbox has been used for the first time in listing actors connected to cybercrime and espionage; the sanction regime targeted 6 individuals and three organizations.[3]

The aim of this thesis is to review the EU Cyber Diplomacy Toolbox, its relation to international law, and the global cyber and economic systems along with the Toolbox's efficiency and proportionality. The diplomacy of the EU's Member States is not completely harmonized, but it is partly like the EU's Common Foreign and Security Policy (CFSP) and now the Toolbox. The thesis analyzes how the Toolbox is applied and what kind of methods it uses in sanctioning. The thesis also looks at the problems that arise in the use of the Toolbox and how decision-making takes place in cases where there is no clear state attribution. It is important to observe the relationship of the Toolbox with international law and the collaboration it requires from the private sector. In addition, the author looks at how the cyber sanctions function in practice and how the principle of proportionality is taken into account in the sanctioning process. After the analysis, the thesis will answer these main research questions: What is the scope of the Toolbox's sanction regime and are the mechanisms proposed in line with the proportionality principle?

The research methodology used in the paper consists of analysis and comparison, and the materials used consist of academic writings on the topic, EU law, analyses of cases, and official EU releases regarding the cyber diplomacy toolbox.

[3] COUNCIL DECISION (CFSP) 2020/1127 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States

2. SANCTIONS AS TOOLS OF INTERNATIONAL DIPLOMACY

The purpose of this chapter is to take a closer look at sanctions in international relations, how they function, and the reasons for their use. It is important to cover these topics since the Toolbox is powered by sanctions in order to achieve established goals. The chapter looks at sanctions in general, and the cyber aspect will be covered in the following chapters of the paper.

2.1 Use of Sanctions

Sanctions can be used for a variety of reasons. One reason is to create a signaling effect to display disagreement with another nation's decisions. For example, the United States used sanctions, including an oil embargo, against Libya in order to demonstrate its opposition to Qaddafi's support of international terrorism.[4] Sanctions have been considered as an alternative to the use of force; in this way, they are used as a coercive tool in order to achieve political aims.[5] Coercive measures are considered more as a punishment and can cause destruction in the targeted nation. The trend is towards more use of sanctions for signaling to reduce intensity in a conflict situation and to not create further hindrances to a resolution.[6] The signaling creates public opposition to a violation of a norm, the aim clearly being to protest against the violation and to make the sanction a symbol of the protest.[7] This means that it serves as a signal to the receiving state and other states and can therefore have an impact that spreads in the form of support for opposition to a norm violation or in the form of awareness of diplomatic intent.

[4] Lindsay, J. (1986). Trade Sanctions as Policy Instruments, *International Studies Quarterly*, 30 (2) 153-173. 166
[5] Ibid., 154
[6] Doxey, M. (1972). A framework of Analysis with Special Reference to the UN and Southern Africa, International Organization, 26 (3), 527-550. 550
[7] Lindsay, J. (1986), *Supra nota 4*, 167

2.2 The Effectiveness and Application of Economic Sanctions

Financial sanctions are one of the Toolbox's key involvement measures. The Toolbox is very new and the result of increasingly complex interactions in cyberspace. Economic sanctions are however not novel. Economic sanctions have been used for quite some time during conflicts or crises for all purposes deemed appropriate at the time by the party administering them. The Toolbox and its sanctions cannot be the subject of thorough investigation, but economic sanctions and their effectiveness, procedures, and reasoning can be evaluated. This chapter focuses on past use of economic sanctions to give an idea of what the effects of imposing financial sanctions for the first time might look like once a sufficient amount of time has passed, in order to evaluate the deterrence and effectiveness of the Toolbox's sanctions. The author considers that the main difference between traditional economic sanctions and the Toolbox's financial sanctions is that the Toolbox's application purposes are cyberspace whereas traditional economic sanctions apply to events taking place in the natural environment, but that their differences are sufficiently limited to enable a comparative analysis.

Evaluating whether financial sanctions are effective can be difficult to impossible since they are closely connected to political, commercial, and security policies. Thus financial sanctions can only be seen as attempts to influence actors in the middle of many other activities.[8] The isolation of the effects of economic sanctions can be completely impossible since the application of sanctions does not occur as a separate incident.[9] Past research on the effects of economic sanctions has generally come to the conclusion that they do not have an impact on the situation, with the exception of a few cases in which they have had a beneficial impact.[10] The Targeted Sanctions Consortium has assessed that UN sanction have most often been successful in imposing constraints, slightly less often successful in sending a signal, and least often successful as coercive measures. The overall success rate of sanctions in achieving their aims is only 22%.[11] The application of EU sanctions is made at the national level by the competent authority. These authorities can work closely together, and the key element is usually information sharing. This is

[8] Hufbauer G. *et al*., (2007). Economic Sanctions Reconsidered, Peterson Institute for International Economics, Washington DC.
[9]Moret, E. (2015). "Humanitarian Impacts of Economic Sanctions on Iran and Syria", *European Security*, 24(1)
[10] Biersteker T. Eckert S. Tourinho, M. Hudáková, Z. *The Effectiveness of United Nations Targeted Sanctions: Findings from the Targeted Sanctions Consortium (TSC)* (Geneva: Graduate Institute of International and Development Studies, 2013). 1-51. 21-23
[11] Targeted Sanctions Consortium (TSC), 2018. Retrieved: https://graduateinstitute.ch/research-centres/global-governance-centre/targeted-sanctions-initiative. Accessed: 17.8.2020.

important since actions such as making reasonable attribution or taking countermeasures need to be in line with international principles such as proportionality.[12] A reason why sanctions are difficult to evaluate on their own is that, for example, UN sanctions are always applied in addition to other measures, never as an isolated effort.[13]

Economic sanctions also have unintended consequences. When economic sanctions are imposed on a nation, this opens the door for third party exploitation, which incentivizes co-operation between major political powers.[14]

An exception to the rule of economic sanctions usually having a low-level impact on a nation or being an insufficient measure in a conflict situation is the case of Nicaragua. The sanctions imposed by the United States against Nicaragua had a large impact on the Nicaraguan economy as a whole. The sanctions were part of negotiations between the two nations in a heavily political situation. The economic development had already been declining in Nicaragua as a result of an insurrection when the Reagan administration cut ties between the United States and Nicaragua. As a result, the sanctions had a heavy impact on the nation which could not be ameliorated.[15]

The examples given in the literature show that it can be extremely difficult to achieve an intended purpose with economic sanctions since they rely on other measures and the development of the situation. The desired purpose or impact seems to most often consist of pressuring or coercing a state to change their policy or behavior in certain situations. Economic sanctions such as those against Nicaragua had a grave impact on the nation due to pre-existing conditions, so they were a final nail in the coffin so to speak. This shows that economic sanctions can have a grave impact if targeted in a manner that interferes with something essential for the sanctioned nation. From a strategic point of view such sanctions might be deemed extremely functional, but in terms of diplomacy there is the argument that a more lenient, less effective sanction is a wiser option in order to reduce the risk of a conflict spiraling out of control. In terms of the Toolbox, this is a valid consideration since travel bans and asset freezes will have a high impact on an individual, but in case that individual is involved in large financial transactions, such sanctions could have a collateral effect on many others. This emphasizes the importance of attribution and evidence collection, which are discussed later in this paper. And

[12] Moret, M. Pothier, F. (2018). "Sanctions After Brexit," *Survival: Global Politics and Strategy*, 60(2), 179-200. 183
[13] Biersteker T. Eckert S. Tourinho, M. Hudáková, Z. (2013). *Supra nota* 10, 40
[14] *Ibid*.,18
[15] Leogrande, W. (1996). Making the economy scream: US economic sanctions against Sandinista Nicaragua // Making the Economy Scream: US Economic Sanctions against Sandinista Nicaragua, *Third World Quarterly*, 17(2), 329-348, 342.

attribution might cause problems since attribution is left to the Member States so the Toolbox's restrictive measures might impact one nation's economy more fiercely than another's, and therefore that nation alone not attributing the attack to an individual might prevent the sanctions from being effective. Countries have the right to deny transit based on the decision of their own competent official, even though the EU can intervene in the decision as well. The point of this analysis is that the decision to impose sanctions on one or more individuals is made from the EU's perspective, but its impact might be suffered far more than individually. When the time comes, the application of the Toolbox is going to be interesting in terms of how these problems are solved or addressed and whether attributions will snowball among the Member States or the mechanism of individual diplomatic decision making will create problems in the system.

3. CYBERSECURITY AND THE EU CYBER DIPLOMACY TOOLBOX

3.1 Cyberattacks against EU cyber targets

Use of cyber weapons is actually not a very recent development. In fact, states have been engaging in cyber operations against each other for over three decades. Stuxnet was a cyber operation in which a computer worm targeted a nuclear facility in Iran. The attack was never officially attributed to anyone, but two countries have been widely suspected.[16] There have been attacks ranging from those on Estonia in 2007 to the WannaCry ransomware attack in 2017.[17] The Estonian attacks were never legally qualified as an attack due to the fact that there was never confirmation of governmental involvement in the attacks.[18] Cyberattacks can have devastating consequences, like in the case of the NotPetya attack, which spread from Ukraine to companies all around the world, causing estimated damages of around 10 billion US dollars.[19]

Wannacry affected over 300,000 computer systems in over 150 countries, using a new method of infection to spread as ransomware.[20] Wannacry demanded ransom payments in Bitcoin, specifically a method called outflow.[21] On Tuesday 27th June 2017, NotPetya started spreading from Ukraine.[22] Using tax software, the malware spread across several sectors of commerce, including the energy industry and healthcare providers. It used a former secret US government program called EternalBlue to spread, much like its predecessor WannaCry. [23]

---

[16] Kivihuhta J. (2018). *Principle of Distinction in Cyber Operations*. (Bachelor's Thesis) Taltech School of Business and Governance Tallinn. 25
[17] Ivan, P. (2019). Responding to cyberattacks: Prospect for the EU Cyber Diplomatic Toolbox, *EPC Discussion paper*, 18 March 2019, 3-13. 3
[18] Kivihuhta J. (2018). *Principle of Distinction in Cyber Operations*. (Bachelor's Thesis) Taltech School of Business and Governance Tallinn. 26
[19] Ivan, P. (2019*). Supra Nota 17,* 4
[20] Turner, A. et al. (2019). A target-centric intelligence approach to WannaCry 2.0, Journal of Money Laundering. 646-665. 648
[21] Ibid., 649
[22] CyberPeace Institute, Case Study: WreckWeb. Dealing With Notpetya. Retrieved: https://cyberpeaceinstitute.org/assets/news-articles/wreckweb_single_page.pdf p 7 Accessed: 17.8.2020
[23] Turner, A. (2019), *Supra nota 20,* 649

Payments made from Bitcoin wallets to fiat currency or other cryptocurrencies made attribution possible at some point where there was enough user information.[24] The fact that the consequences can be this harsh for a market, not to mention individual companies, is a cause for concern. The efforts to block this activity can be seen at many levels, including legislators creating legal definitions for illegal activities in cyberspace and antivirus software sold to consumers, but it is a different matter to deal with these sorts of malicious operations on a larger scale.

3.2 International cybersecurity and the EU

In order to look at the elements of the Toolbox, the basic elements of its surroundings need to be reviewed. The EU Member States have committed themselves to the Common Foreign and Security Policy[25] (CFSP), and as a part of that, the more active Common Security and Defense Policy, through which the EU is able to take part in crisis management.[26] These EU initiatives derive their essential principles from international law.

There are international efforts to bring clarity to regulation and create a foundation for cyberspace. One of these efforts is the United Nations Group of Governmental Experts (UN GGE from now on). According to the norms created by UN GGE, states should take better care of their ICT infrastructure and make sure that harmful actions are detected and prevented within their territory. States should also work towards a global culture of cybersecurity and should consider working together with other states and should create possible responses to aid another state whose ICT infrastructure has been compromised. This creates an international effort towards combatting cyber threats or at least a loose framework in which states can begin to create a legal and diplomatic approach to the issue. These are the current international efforts to clarify a legal framework and legal procedures in cyberspace.[27]

[24]Ibid., 650
[25]Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union 2012/C 326/01, Article 36
[26]Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union 2012/C 326/01, Article 38
[27] UN GGE: Efforts to Implement Norms of Responsible State Behaviour in Cyberspace, as Agreed in UN Group of Government Expert Reports of 2010, 2013 and 2015. Retrieved https://www.un.org/disarmament/wp-content/uploads/2019/12/efforts-implement-norms-uk-stakeholders-12419.pdf Accessed: 17.8.2020

The EU has become more involved in cybersecurity and is beginning to have a bigger impact on the field.[28] Focusing on the specific case of cybersecurity, Carrapicco and Barrinha conclude that the EU is ambitious in attempting to achieve a role as an important and coherent cybersecurity actor. The political importance of cybersecurity and efforts to consolidate it in a progressive manner are both quite recent, and the EU has shown signs of moving in this direction.[29] The coherence of a cybersecurity strategy is measured not only by efficiency, but also by participation and accountability. The EU must also defend the values it holds highest while acknowledging that decision making in cybersecurity is characterized by a lack of transparency.[30]

In the current atmosphere there is a need for the EU to take charge of cyberspace as well. Cyberspace has created the necessity to have tools for international relations, and the EU has created the Toolbox to answer the new challenges.

The Toolbox is essentially a part of the European Union's ways of tackling and dealing with difficult situations that occur in cyberspace. These can vary from espionage to hostile attacks against a hospital network.[31] How to deal with these situations is not easy, and therefore the Toolbox has been introduced as a part of the EU's Common Foreign and Security Policy.

The EU has already previously taken measures to combat crime in cyberspace.[32] The task of combatting cybercrime arose in 2015 when the Council declared that there needs to be a mechanism to mitigate and deter cyber threats in the EU, which is what the Toolbox will start to do.[33] The deterrence will work as a long-term preventive measure against malicious cyber activity. The initial EU releases to create the Cyber Diplomacy Toolbox were preceded from March 2017. On the 19th of June 2017, the Council decided to enforce the new policy instrument that is known as the Cyber Diplomacy Toolbox.[34] The decision was based on the Treaty on European Union and in particular Article 29. The proposal to implement the instrument came

[28] Wessel, R. (2015). Towards EU Cybersecurity Law: Regulating a New Policy Field, IN Tsagourias, N. Buchan, R. (eds) Research Handbook on International Law and Cyber Space (Cheltenmham Edward Elgar Publishing) 403-425
[29] Carrapicco, H. Barrinha, A. (2017). The EU as a Coherent (Cyber)Security Actor? *Journal of Common Market Studies*, 55(6) 1254-1272, 1267
[30] Bendiek, A. (2012). European Cyber Security Policy, *SWP Research Paper No. 13* Available: https://www.swp-berlin.org/en/publication/european-cyber-security-policy/ Accessed 9.7.2020
[31] Brandom, R. (May 12th 2017). UK hospitals hit with massive ransomware attack, *The Verge*
[32] *Ibid.*
[33] European Parliament and Council of the European Union,"Directive 2016/1148 of the European Parliament and the Council concerning measures for a high common level of security of network and information systems across the Union", Brussels, July 7, 2016.
[34] Council of the European Union, Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox") Brussels, 7 June, 2017.

from the High Representative of the Union for Foreign Affairs and Security Policy. It was a response to malicious cyber activities. On 11th of October 2017, guidelines were implemented for the CDT and then approved by the Political and Security Committee. In June 2018 the Council adopted a conclusion that stressed that the Union needs to develop cyber capabilities against threats coming from outside the Union as a predecessor to the final decision on the Toolbox. The Council decision on 16th of April 2019 condemning malicious cyber activity against ICTs was the final Council decision leading up to the Toolbox.

3.3 The EU Cyber Diplomacy Toolbox

The aforementioned preparatory procedures led to Council decision 2019/797 of 17th May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States. Council Regulation 2019/796 was the implementation of the preceding decisions on the Cyber Diplomacy Toolbox. The decision is focused on attacks that are against the Union and pose a major threat to the Union. The cyber-attacks that form a major threat to the Union are created outside the Union and are based on infrastructure outside the Union. They are carried out by any natural or legal person, entity, or body outside the union. The cyber-attacks involve elements of one or more of the following: access to information systems, interference with information systems, data interference or interception.[35] The significance of an attack is determined by analyzing its scope, scale, impact and disruption, number of persons or entities affected, how many states are concerned, economic loss suffered by targets and the economic benefit of the perpetrator, and the amount of data stolen or breached. Attacks mainly target critical infrastructure and services that maintain vital economic activity or critical state functions. First, the sanctions enable an EU Member State to prohibit entrance into their country from a natural person who is responsible for a cyber-attack. Also, the EU can prohibit entrance from natural persons who aid cyber-attacks. Secondly, natural persons or an entity or body can have their assets frozen in the EU if they are linked to a cyber-attack. [36]

The sanction regime has a clearly established scope for defining malware by first checking the requirement of an external threat. These external threats originate, or are carried out, from outside the Union and use infrastructure outside the Union. The sanction regime is applicable if the attacks are carried out by any natural or legal person, entity, or body established or operating outside the Union or are carried out with the support, at the direction, or under the control of any natural or legal person, entity, or body operating outside the Union. A person who is within the

[35] Botek, A. (2019). European Union establishes a sanction regime for cyber-attacks, INCYDER Database, The NATO Cooperative Cyber Defence Centre of Excellence. Retrieved: https://ccdcoe.org/library/publications/european-union-establishes-a-sanction-regime-for-cyber-attacks/ Accessed: 17.8.2020

[36] Ibid

EU territory but is working for a government outside the EU also falls under the scope of the guidelines.[37]

Listing and delisting of the Toolbox is done based on the Council's decision and due to the Council's composition, so the decisions are political in nature. The decision to sanction has to be unanimous to ensure that the Member States comply with the decision. [39]

The restrictive measures also need to have a transparent and efficient method way of de-listing, in order to maintain integrity in the procedures. This is done in case there have been mistakes in the analysis of the evidence according to which sanctions have been imposed, there is new evidence available, or there is a change in relevant facts.[41]

The Member States have to appoint competent authorities to enforce the sanctions, who can also lift specific sanctions for specific persons if, in their analysis, it is justified to do so. Even though they have the right to exempt persons from the travel bans in their own jurisdiction, the Council can still annul their decision. The competent authorities can also moderate the sanctions imposed by the Council.

There are also the deterrence effects that the sanctions create, which prevent future attacks by posing a threat to criminals. However, the sanctions also create deterrence effects that prevent future attacks by threatening criminals with consequences. The US has already imposed sanctions against multiple non-state actors and has put their names on a blacklist, including the directors of the GRU, FSB, and Iranian intelligence agencies. The US sanction regime is simpler and more effective since it does not depend on a unanimous decision.[42] The EU has however reacted to cyber threats by creating the Toolbox.

The EU's Common Foreign Security Policy provides a framework for responding to threats from abroad. This means that sanctions can be imposed in order to achieve the following objectives of the EU treaties: safeguarding the EU's values, security, independence, integrity, supporting democracy, rule of law, human rights, the principles of international law, and preventing conflicts. The cyber activities addressed in the Toolbox are limited to ones with significant

[37]Council Decision 2019/797 considering restrictive measures against cyber/attacks threatening the Union or its Member States

[39] Pawlak, P. Biersteker, T. (2019). Guardian of the Galaxy, EU cyber sanctions and norms in cyberspace, *Chaillot Paper 155*, October 2019, European Institute of Security Studies, Paris, 1-103, 38

[41] Council of the European Union, Restrictive Measures (Sanctions) – Update of the EU Best Practices for the Effective Implementation of Restrictive Measures, Brussels, 4 May 2018. ref. in. Pawlak, P. Biersteker, T. (2019). Guardian of the Galaxy, EU cyber sanctions and norms in cyberspace, *Chaillot Paper 155*, October 2019, European Institute of Security Studies, Paris, 1-103, 38

[42] Botek, A. (2019), *Supra nota 35*

consequences and that involve accessing systems with important information. The regime also covers attacks against the Union's institutions and its delegations to third countries and international organizations.[43] The Member States are expected implement certain measures in accordance with the Toolbox. They should prevent entry, transit, or freeze all financial assets of the people who are responsible for cyberattacks that violate the criteria mentioned above.[44]

[43] Pawlak, P. Biersteker, T. (2019). *Supra nota* 39, 35
[44] Botek, A. (2019), *Supra nota 35*

4. LEGAL CHALLENGES

4.1 Attribution and the EU Cyber Diplomacy Toolbox

The aim of this chapter is to try to bring clarity into what exactly is the problem in attribution and malicious cyber activity. The EU sanction regime has not sanctioned states for malicious cyber activity, only individuals and private entities, which is a little strange since such activity against the EU member states is generally known to require state level support. The following parts of this chapter aim to explain attribution in the context of international law.

There are different definitions of attribution. Technical attribution means the attribution of an attack to a party using technological methods that analyse the information left from or discovered about the attack. All source attribution however takes into account other information as well, not just technical, so the information used to make a judgement on the situation does not provide certainty of proof.[45]

"Cyber attribution is the process of tracking, identifying and laying blame on the perpetrator of a cyberattack or other hacking exploit".[46] A fundamental problem in attribution is identification of the hostile party from the point of view of responding. In terms of the sanction regime, this poses a major challenge. In the EU diplomatic system, attribution is still up to the Member States, so the EU institutions only have an advisory role. The role of the EU institutions in political judgement is however key when determining the cyber sanctions.[47]

The term attribution means connecting an act or operation to one or more specific individuals, groups, or states. Attribution can be direct or indirect. Direct attribution means the identification of the individuals carrying out a hostile operation and identification of the state under whose instructions the individuals acted. Indirect attribution means that a state is not involved but could

[45] Lin, H. (2012). Dynamics and Conflict Termination in Cyberspace, *Strategic Studies Quarterly*, 6 (3) 46-70. 49
[46] https://searchsecurity.techtarget.com/definition/cyber-attribution Definition: cyber attribution
[47] Mejia, E. (2014). "Act and Actor Attribution in Cyberspace: A Proposed Analytic Framework." *Strategic Studies Quarterly*, 8(1), 114–132. 118

be aware of the activity and does not prevent it.[48] The Council Decision and Regulation have provided criteria for listing individuals or entities in this context. The Council Decision is abundantly clear in that cyber sanctions imposed in the context of the regulation and decision should be differentiated from state made diplomatic statements and sovereign political decisions.

Attributing a cyber operation implies 3 different dimensions: firstly, identification of the computers and networks that were used to conduct the operation; secondly, linking the operations to its human perpetrators; and thirdly, ascertaining the potential wrongdoing of a state if the perpetrator did act on behalf of a state.

States can act through individuals and entities that have no clear ties to the state, meaning for example that the state has no institutional or organizational connections with the perpetrators. This is important in terms of attribution. In the context of the law of state responsibility, two criteria must be fulfilled: Firstly, the act is attributed to the state; secondly the conduct constitutes an internationally wrongful act.[49] The key is to attribute a certain action to a state in case the goal is to set certain sanctions. The mere fact that a cyber operation is conducted from a state by citizens of that state is not sufficient to prove state involvement.[50] To make matters worse, attributing an attack is a slow and arduous process.[51] However, attribution cannot be handled at all times with this level of stringency. Some argue that states should lower their threshold for attributing cyberattacks, especially in cases where there is an armed attack at the same time.[52] The complexity of determining perpetrators in cyberspace has given an image of impunity to states, and the lack of identification of an attacker creates difficulties for responsive measures.[53]

The current legal framework of tracking and verifying the origins of events is such that criminal law's requirement of proving guilt beyond any doubt is not does not exist in international law. In other words, the development of standard of proof seems to be taking the direction that proof is less and less needed.[54] The legal experts of both the UN GGE and the Tallinn Manual 2.0 are

---

[48] *Ibid.*
[49] Schmitt, M. (2013). *Tallinn Manual on The International Law Applicable to Cyber Warfare*. Cambridge University Press, p 29.
[50] Pawlak, P. Biersteker, T. (2019). *Supra nota* 39, 54
[51] Mudrinich, E. (2012). Cyber 3.0: The Department of Defense Strategy for Operating in Cyberspace and the Attribution Problem. *Air Force Law Review, 68,* 167-206. 172
[52] Allan, C. S. (2013). Attribution issues in cyberspace. *Chicago-Kent Journal of International and Comparative Law, 13(2),* 55-83. 82
[53] Schmitt, M., Vihul, L. (2014). Proxy wars in cyberspace: The evolving international law of attribution. *Fletcher Security Review,* 1(2), 53-72. 54
[54] Tolppa, M. (2018). *Standard of Proof in Attribution of Internationally Wrongful Cyber Operations,* (Master's Thesis) Taltech School of Business and Governance Tallinn, 59

leaning towards the idea that there is an obligation for the injured state to have evidence, even though this type of evidence is rarely disclosed.[55] Identifying and proving state involvement would be nearly impossible using requirements of criminal law. Some argue that proof beyond reasonable doubt should be sufficient instead of proof beyond any doubt.[56] The fact remains that attribution made on the state level does not follow any court's legal procedure and therefore it can be difficult to develop a widespread practice concerning standard of proof.

Attribution has been used in some past cases to implicate actors and states behind attacks. Many governments nearly simultaneously attributed the Wannacry attacks to North Korea and the Notpetya attacks to Russia.[57]

Attribution is extremely important so that there can be a collective response to and interpretation of a situation. In practice, attribution has become difficult since collaboration between different levels of competence within states has changed drastically with the development of cyberspace and since co-operation and collaboration between the sectors of Member States vary within the EU.[58] Different EU Member States have very different approaches to cyber operations, making it difficult to achieve joint responses. When it comes to potential collective responses, it is important that they comply with international law. On the other hand, self-defense is also a legitimate response.[59] The UN document Responsibility of States for Internationally Wrongful Acts in Chapter II gives states the right to use countermeasures as a response to wrongful acts but gives this right only to a single state. [60] Retorsion can be carried out as a community response but countermeasures can only be performed by a single sovereign nation. The victim state can still receive aid from other states even though the other states cannot engage in the conflict or participate in countermeasures with the attacked nation. It is important to notice that this can lead to a situation where the retorsion and countermeasures can be coordinated at the EU level. Countermeasures can only be applied by one nation.

State procedures regarding cyber evidence vary, and this happens for a few reasons. Firstly, concrete evidence can be difficult to ascertain and validate. Secondly, if such evidence is found,

---

[55] Ibid., 36
[56] Shackelford, S. J., Andres, R. B. (2011). State responsibility for cyber attacks: Competing standards for growing problem. *Georgetown Journal of International Law*, 42(4), 971-1016. 1014
[57] Botek, A. (2019), *Supra nota 35*
58 Boeke, S. National cyber crisis management: Different European approaches, Governance, an international journal of policy, administrations and institutions, 31(3), 449-464. 449
[59] Dupont P. (2012). "Countermeasures and Collective Security: The Case of the EU Sanctions Against Iran", *Journal of Conflict & Security Law*, 17 (3),301-336. 322
[60] Responsibility of states for international wrongful acts, Chapter 2 Article 49 (1) https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf Accessed: 9.92020

it can be sensitive information vital to the state's national security and is therefore never made public.[61] This practice however might run into problems in the future since the international community has grown more demanding on having concrete evidence regarding attribution. The UN GGE 2015 Report reflects this issue.[62]

When it comes to attribution, there are different levels and topics to cover. Attribution can consist of technical attribution to the systems and hardware used or can consist of personal identification of the person operating the system. Technical attribution to the host of the attack is easier than to the person carrying it out. There are a few reasons for this. Even though a person can remain anonymous while conducting operations in cyberspace, some data is always left behind which makes it possible to later locate connected places and systems. When it comes to identifying a specific person at a location, certainty is naturally far more difficult to achieve. [63]

Attribution exists at three different levels of identification, which also result in higher levels of proof. An increasingly higher level of attribution is required depending on whether it is needed for a national security issue, civil suit, or criminal suit. At the first level, there must be identification of a cyber weapon so that it can be clearly stated that a crime has taken place and what the characteristics of the attack are and what was used to conduct it. This is vital for a criminal suit since without this there can be no further criminal investigation into the matter. At the second level, the origin of a malicious attack can be tracked to the infrastructure of a state and often narrowed down to a region or city. At the third level is the identification of a criminal or organization behind the attack, which enables attribution of an attack to a natural person or persons. The level of certainty and evidence that is required can also depend on the severity of the attack. The Budapest Convention on Cybercrime provides classifications and legal tools to enable nations to deal with domestic cybercrime. It also aims to improve international co-operation and collaboration to protect societies from cybercrime.[64] The described three levels are used consecutively as three required steps in criminal law, but not international law.

The legal issue of proof is heavily dependent on attribution and its certainty. Proof in analyses of cyber incidents can consist of a range of probabilities. The requirements for proof in domestic

---

[61] Pawlak, P. Biersteker, T. (2019). *Supra nota* 39, 59

[62]United Nations General Assembly (UNGA), "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," July 22, A/70/174, 2015. 1-17. 13

63 Shamsi, J. et al. (2016). Attribution in cyberspace: techniques and legal implications, *Security and Communications Network*, 9(15), 2886-2900. 2889

[64] *Ibid*., 2890

courts depend on whether the matter is handled in a criminal or civil procedure.[65] In international law, the situation is clearly different. As stated before, there is no clear judge for the world to make the decision of who is considered responsible for malicious acts. The diplomatic side of attributing an attack does not have a unified standard for attribution nor is the criteria for attribution domestically the same or regulated in the same way as domestic legal procedures are.

The question of attribution has been in the spotlight regarding reasonable consequences for malicious activity in cyberspace. The reality is that the decision made on attribution is diplomatic in nature and therefore the political and legal considerations are not that easily separated from the entire process.

In terms of attribution, proportionality is partly relevant and partly not. Attribution is made or not, and strictly it is not a question of proportionality. However, proportionality is important when the evidence is being evaluated. It is unclear whether a standard similar to that used in civil law or criminal law is applied. Problems can occur since clear standards have not been set, for instance proof beyond reasonable doubt, preponderance of the evidence, or rules on burden of proof. Also, the information gathered to achieve attribution must be legitimate, and suitable to achieve the aim. In addition, information should be gathered within the limits of reasonability from the parties involved. A problem that can occur in this scenario is that since some of the information is kept secret for state security reasons, the methods or evidence may never see the day of light. Thus, proportionality would only be a possible? value that is followed or not without control. Because these are international political and diplomatic relations or conflicts, there is no clear legal procedure to confirm that proportionality is followed.

In the next chapter the author will review the scope of the Cyber Diplomacy Toolbox and the proportionality of its response, doing this from different angles by comparing it to international law and reviewing how it can be made more effective in the future.

4.2 International Law and the EU Cyber Diplomacy Toolbox

[65] *Ibid.,* 2890

International law consists of different bodies of rules that give structure to interactions between nation states. They are the result of international co-operation that has become customary in international conduct or international agreements. Economic interaction among states is extremely important.[66] The generally noted problem with international law is that the structure is decentralized and therefore the efficiency of the rules is questioned. The system essentially does not offer for legal power over states but a system where states can agree on matters or seek intervention voluntarily or use the later discussed tools against another state. Essentially international law cannot forcefully control the conduct of states, and there is no court that has jurisdiction over the international community.[67]

Cyberspace has developed rapidly in the past years, and the constant presence and frequency of cyberattacks has surpassed the international community's political ability to respond.[68] International law has provided indications for a code of conduct in cyberspace, providing laws stating what is permitted and what is not. International law principles involve prevention of transboundary harm, which in essence means that no state should knowingly allow their infrastructure to be used against another state.[69] The Toolbox supports this principle. The toolbox also supports the other principles of international law and applies them to cyberspace. The Toolbox also has protective elements for states' laws by providing rules for legitimate cyberspace activity. In case a state is put in a situation where it is necessary for it to react to hostile cyber operations, international law provides these four different kinds of responses: retorsion, countermeasures, self-defense, and jus ad bellum.[70] This paper deals with retorsion, countermeasures, and self-defense.

Retorsion measures are generally speaking unfriendly reactions to unfriendly actions. Unfriendly acts as acts of retorsion are not illegal.[71] Retorsion is essentially a lawful but unfriendly measure that states can take. Such measures include cutting cyber transmission coming from another state on the basis of sovereignty over the territory to which it is transmitted. Retorsion is distinguished from countermeasures by the fact that acts of retorsion are always legal whereas

[66] Henderson, J. (1986). Legality of economic sanctions under international law: The case of Nicaragua. *Washington and Lee Law Review*, 43(1), 167-196. 168
[67] Ibid., 169
[68] Anderson, T. (2017). Fitting virtual peg into round hole: Why existing international law fails to govern cyber reprisals. *Arizona Journal of International and Comparative Law*, 34(1), 135-158. 136
[69] 19. Ryan, D. *et al*. (2011). International cyberlaw: normative approach, *Georgetown Journal of International Law*, 42(4), 1161-1198, 1182
[70] Anderson, T. (2017), *Supra nota 66*, 142
[71] Ibid., 143

countermeasures would be illegal as initiative acts.[72] Countermeasures would normally be unlawful but when they are used as a proportional countermeasure they can be legal. Countermeasures can be legal as a response to a failure to fulfil international obligations.[73]

According to one interpretation, a state is defenseless against attacks that do not qualify as something that can be responded to with countermeasures. This is a dangerous idea. It increases the possibility of a situation escalating into an armed attack.[74] Countermeasures offer states options to respond to attacks in a more aggressive manner than retorsion and thus do not force them to resort to an armed attack. Countermeasures are still subject to limitations, the most important of which is that countermeasures are only available against states. If a malicious operation is initiated by a non-state actor, the state that is targeted is not allowed to use countermeasures against private, non-state actors. In previous cases, the countermeasures had to cause harm to another state, not to a private actor.[75] However, in the discussions of the Tallinn Manual 2.0, the experts did not agree that only states should be lawful targets for measures in case a group or an attack continues to cause harm.[76]

A further limitation is that countermeasures must be solely carried out by a single state. Even if there is a friendly state that could engage in the countermeasure along with the initiating state, this would be against international law. Regardless of these safeguards and limitations, a state that takes countermeasures does bear the risk of the situation escalating into an armed attack.[77]

The next higher, third measure is reprisal. Reprisal is otherwise similar to a countermeasure in that it would be illegal during most situations except as response, but reprisal has an element of coercion in it. Self-defense can be a cyber operation or some use of military force in response to an attack. There is no specific definition as to when a cyberattack is considered an armed attack.[78]

[72] Schmitt, M. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. - *Cambridge University Press*, p 112
[73] Anderson, T. (2017), *Supra nota 66*, 147
[74] Schmitt, M. N. (2014). Below the threshold cyber operations: The countermeasures response option and international law. Virginia Journal of International Law, 54(3), 697-732. 730
[75] Ibid., 731
[76] Schmitt, M. (2017). *Supra nota 72*, 114
[77] Schmitt, M. N. (2014), *Supra Nota 74*, 730
[78] Anderson, T. (2017), *Supra nota 66*, 149

International law is especially complex because each state interprets it differently. This can result in efforts to seek a more unified approach or it can push states apart due to different interpretations and create new problems.[79]

The proportionality principle covers all legal considerations in EU law and is ultimately derived from international legal principles. In EU law this has been implemented in that there must be a legitimate aim for a measure. The measure and its aim must be sound and must take evidence review into consideration. The measure must also be necessary to achieve what it is set to accomplish, while being reasonable towards other parties involved with the given situation.[80]

4.3 Due Diligence in Cyberspace

In this chapter the author introduces another principle of international law, due diligence. The concept of due diligence in cyberspace has been discussed by Luke Chircop in 2018.[81] The principle of due diligence aims to bring clarity to two important problems in cyberspace. Firstly, do a nation's capabilities determine its responsibility for cybercrimes originating in its territory? Secondly, how much does cooperation between states affect their responsibility for each other regarding information and prevention of cybercrime? From the EU's point of view, international law is an important part of security in cyberspace. Since international law is a pillar of rule-based international order, it is vital that international law be a key part of cybersecurity. Due to the importance of international law, it is not surprising that the core of the EU's cyber diplomacy is the prevention of cybercrime and hostile cyberoperations.[82] The decision to make due diligence an intrinsic part of the cyber diplomacy toolbox has strengthened the EU's aim to empower this principle in their approach to cyberspace.[83]

According to the principle of due diligence, a sovereign state has the right to its territory, but it also has the obligation to maintain its territory and not allow it to be used against the sovereign

[79] Tikk. E. "Will Cyber Consequences Deepen Disagreement on International Law," *Temple International & Comparative Law Journal 3*2(2) (Summer 2018): 185-196. 195
[80] Craig, P. de Burca G. EU LAW, Text, Cases and Materials. Fifth Edition. 526
[81] Chircop, L. (2018). A Due Diligence Standard of Attribution in Cyberspace, *International & Comparative Law Quarterly*, 67(3), 4
[82] Council of the European Union, *Council Conclusions on Cyber Diplomacy*, Brussels, February 11,. 7.
[83] Shackelford, S. Andres, R. (2011). State responsibility for cyber attacks: Competing standards for growing problem. G*eorgetown Journal of International Law*, 42(4), 971-1016. 1014

rights of other nations.[84] States have the obligation to exercise due diligence, which means that if they encounter harmful action carried out in their territory against another state, they have the responsibility to intervene in the situation.[85]

Instead of classifying the crime that has taken place, emphasis could be on the state's activity. Could the state have done something better or could the entire situation have been prevented? In case a sovereign state is aware of malicious cyber activity in their territory against another state and does not take any action to prevent this, they are in violation of the due diligence principle.[86] This means that the nation that has been targeted by the malicious cyber activity can take measures against the individual actor or the state in which the actor is. Emphasis on due diligence responsibilities can make collective attribution easier. This is because if a state has not fulfilled their due diligence duties, the standards of attribution are lowered. The due diligence responsibility of the state is independent of the question of who has committed the acts, of what entities or individuals carried them out and whether due to nationalistic interest or otherwise hostile intent towards another state or whether only to gain commercial information. If a nation has not exercised due diligence, it is easier to diplomatically attribute to them the responsibility for the malicious actions. So, the state's lack of due diligence is what matters, not who has been behind the malicious activity. If the state knew, or could have known, about the activity, the state is responsible due to its negligence in preventing or stopping the activity. Due diligence is important because the state can be seen as responsible if the malicious activity took place within its infrastructure. The due diligence requirement is not absolute, however; clear steps taken to fulfil this requirement are sufficient, and a single cyberattack cannot be interpreted as a state having not acted responsibly.

The principle of due diligence and its application to cyberspace due to the EU's Cyber Diplomacy Toolbox is a foundational step in legal and diplomatic developments that can have global consequences. As stated above, the requirement to exercise due diligence is not merely a requirement to not engage in cybercrime and instead demands the responsibility of countries to engage in in cyber activities so that they can prevent such operations from taking place in their nation. The EU is at the forefront of the application of the due diligence principle in order to

[84] Schmitt, M. (2017), *Supra nota 72,* 30
[85] Ibid. 72
[86] Roscini, M. (2014). *Cyber Operations and the Use of Force in International Law* (Oxford: Oxford University Press, 87

show an example to the global community of the application of due diligence and the resolve to act in accordance with it.

4.4 Cyber sanctions and the private sector

Cyber diplomacy has an impact on more than the relations between governments; it also has an impact on the market, which directly affects the private sector. The use of cyber sanctions such as travel bans or asset freezes includes technological solutions, and they function a lot more efficiently when there is fluent cooperation between the private sector and states. The sophisticated machinery that the private sector has plays a big part in the process of acquiring information for the decision makers. There is of course a difference in interest when such information is gathered by the private sector. Governments are interested in the person that carries out illegal activity whereas the private sector is mostly concerned with protecting its business and commercial interests.[87]

False attributions or claims are a lot more damaging for governments than for the private sector. This is why governments need to be wary of false information and insufficient information that might damage their relations with third countries.[88] In addition to norms having been defined by governments, the private sector has taken up the task to set norms for its own behavior in cyberspace.[89] There are many reasons for this, but mostly because the private sector is creating an environment of financial prosperity, and creating a responsible environment is a driving force behind developing a company's business. It benefits businesses to keep cyberspace in better order because all malicious activity, including state affiliated cyber operations, have a negative impact on business. Suspicions about the activities of governments in cyberspace make business more costly. Company-created norms have developed quite fast and have led to cooperation between the private sector and states. The 2018 Paris Call for Trust and Security in Cyberspace was a collaboration between Microsoft and the French government, and it was endorsed by the EU Commission and had over 500 signatories. It is a mix of UN-driven normative politics and

[87] Pawlak, P. Biersteker, T. (2019). *Supra nota* 39, 70
[88] Romanosky, S. (2017). "Private-Sector Attribution of Cyber Attacks: A Growing Concern for the U.S. Government?", Lawfare, December 21, 2017. Retrieved from: https://www.lawfareblog.com/private-sector-attribution-cyber-attacks-growing-concern-us-government, Accessed: 12.8.2020
[89] Eggenschwiller, J. (2019). International Cybersecurity Norm Development: The Roles of States Post-2017", *Research in Focus, EU Cyber Direct*, March 2019, 1-11. 9

bottom-up approaches. The Paris Call has accepted the idea that sustainability as well as resilience to and prevention of criminal cyberactivity is of great importance. It is also of utmost importance to protect the integrity of the internet and its accessibility.[90]

Interventions are used by companies that can prevent the use of certain tools or applications or can restrict access to servers. This activity is not included in the toolbox. An example of this type of activity is how Facebook increased their efforts to block users that tried to affect the election and spread hate speech. This type of private sector sanctioning might be as important as political sanctions in the future.[91]

One of the most common tools for criminals are botnets, networks of computers spreading malware or attacking a target. These programs allow criminals to use computers remotely and coordinate larger attacks.[92] The private sector plays an intrinsic role in taking botnets down due to its technological capabilities, such as Microsoft taking legal action against the Waledac botnet.[93]

The private sector in cyberspace has become more than a party playing by the rules of governments. The private sector is essential in the technological aspect of fighting cybercrime and also has shown its ability to have a sanctioning regime of its own. “Sanctioning” by the private sector is not legally based but done based on business interests. The EU is asking the private sector to comply with the rules of the Toolbox on sanctioning. Private companies have the power to block operators from their networks and create the norms for responsible behavior in cyberspace. Even though this does not have a direct effect on the EU sanctioning regime, it can have a great impact on the level at which the sanctioning power can function. These normative initiatives from the private sector create a context for sanctioning in cyberspace and its application, especially if there is universal recognition of the need for sanctioning.[94]

It seems to be quite inevitable that the Toolbox will affect the private sector and that this will increasingly apply the Toolbox since there are many private actors on the internet and they run many online services. In terms of the future, the author considers that there is not much sense in wasting resources to develop public capabilities that already exist in the private sector. An increased role of the private sector in cybersecurity might not arise merely due to cooperation

[90] Ibid.
[91] Pawlak, P. Biersteker, T. (2019). *Supra nota* 39, 75
[92] Eichensehr, K. (2017). Public-private cybersecurity. Texas Law Review, 95(3), 467-538. 479
[93] *Ibid.*
[94] Pawlak, P. Biersteker, T. (2019). *Supra nota* 39, 77

and collaboration since there is a tendency for those who have capabilities to begin to recognize their position and this may lead to a more privatized version of diplomacy merely due to the fact that the private sector would be the one doing all the heavy lifting. The outcome might not be that bleak, but the due to the development of the internet, the world is moving towards a more corporately influenced system and this might just be a result of the increased economic influence of the private sector, which is therefore taking a bigger role in the field. Additionally, the norms developed in the private sector might become more influential in the future because it is their everyday life to deal with threats first hand and leave the bigger things to be decided by the those who are legally in power. It depends on how the situation is looked at, but in the Union there is the principle of subsidiarity, which a bit broadly expressed says that decisions are best made at the closest level to where the problems are. Therefore, private sector norms might have more practical application and impact than the principles developed by the EU since the former need to be applied immediately in order to keep economic activity going.

5. IMPLEMENTATION AND PRACTICE

5.1 Practical aspects of cyber sanctions

The chapter is focused on the practical application of cyber sanctions. One of the aspects that is extremely important to ascertain is how a cyber sanction is going to affect cyberspace in reality. It is important to know how one can avoid activity leading to sanctions and how the sanctions affect the way cyberspace functions. The problem with sanctions is that it is not always completely predictable how their effects are going to play out. There can be complex consequences of sanctions, some of which are a side effect of the main intentions, and even the main intentions can produce consequences that were not within the original intention. Even when unintended consequences occur, there is a necessity to apply the sanctioning regime. There needs to be a balance between the harm prevented by the sanctions and the harm caused as a result of applying them.

When there is malicious cyber activity coming from outside the borders of a country, Mutual Legal Assistance Treaties (MLAT) help determine the threats and persons involved in order to avoid unnecessary difficulty in gathering information. The cooperation of investigation between countries requires both to take into consideration their legal processes.[95] There is also a need for trust between the different countries' police forces so that the information provided can be acted on or used as a part of the investigation. Unfortunately, there is always a delay in the investigations as a result of due process and standard of proof. This is not to say that these are a problem in the sense that they are necessary to ascertain reliable proof and a prosecution based on that. The problem arises from cyberspace having geographical flexibility and the evidence being in the jurisdictions of several nations, which is bound to cause hindrances in the investigation process.[96]

[95] Gurkaynak, G. Yilmaz, I. Taskiran, N. (2013). Governmental Efforts and Strategies to Reinforce Security in Cyberspace, *International Law Research*; 2(1), 185-194. 187

96 Osula, A. (2015). Mutual Legal Assistance & Other Mechanisms for Accessing Extra Territorially Located Data, *Masaryk University Journal of Law*, 9(1), 43-64, 46-50

If there is a lack of cooperation between the police forces of different nations, there is not much possibility of immediate action being taken by the investigating party. One possibility is to wait for the criminals to travel outside their country and arrest them then. Travel bans have a negative effect in the sense that if a criminal is banned from traveling as a result of applying the Toolbox, they are less likely to be caught during travel, making the practical efforts to catch them more difficult. These cases become even more difficult when there is political friction between nations; the application of legal sanctions to criminals can be difficult if there is no co-operation. There is trend that the attacks are usually coming from nations with which there is no Mutual Legal Assistance Treaty.[97]

Cryptocurrencies are a current topic, and there are many aspects to their benefits and downsides. One of the unfortunate aspects is that cryptocurrency benefits criminals in their attempts to avoid legal consequences. The access to the international banking system can be restricted, which can encourage attempts by nations who are restricted to conduct attacks in order to steal funds. There are multiple ways in which these are conducted, but the attacks can be organized to mask a transaction as an in-person withdrawal, or in the case of cryptocurrency, the funds can be transferred without the parties being known to outsiders.[98] Governments and the private sector are increasingly committed to finding out how criminals use cyber tools that allow them to avoid sanctions.[99] Companies and individuals who participate in cryptocurrency exchange are not exempted from the basic requirements and laws governing financial activity. The decentralized system of cryptocurrencies allows persons to engage in financial activity without being recognized, which then allows them to engage in global financial activity without any participation from the banking sector.[100] The compliance department of banks can restrict an individual's access to financial transactions when they operate within the banking system. However, cryptocurrencies are out of their reach in terms of restrictions and background checking the person behind a transaction. Private networks allow people to complete transactions that would otherwise be recognized as sanctionable due to detection or knowledge of the parties involved. There is no accurate data on how much cryptocurrencies are a part of sanction evasion, but there are predictions that this criminal activity is on the rise and that the future might bring

[97] The Center for Internet and Society, Stanford Law School, Gail, K. (2015). The Mutual Legal Assistance Problem Explained [Blog Post] Retrieved: http://cyberlaw.stanford.edu/blog/2015/02/mutual-legal-assistance-problem-explained Accessed: 12.8.2020
[98] Higbee, A. (2018). The Role of Cryptocurrency in Cybercrime, *Computer Fraud & Security*, July 2018, 14
[99] Pawlak, P. Biersteker, T. (2019). *Supra nota* 39, 81
[100] Reddy, E. Minnaar, A. (2018). CRYPTOCURRENCY: A TOOL AND TARGET FOR CYBERCRIME, *Acta Criminologica: Southern African Journal of Criminology* 31(3), 71-92. 73

problematic situations enabled by cryptocurrency technology. There are concerns about sanctioned states like Russia, Venezuela, and Iran building blockchain technology that allows them to engage in transactions in the financial world outside the reach of sanctions.[101]

Holding on to sanctions and complying with regulations and sanctions is important for the main operators in the world of cryptocurrency. The financial sector or mostly the banking sector is incapable of detecting allowed or prohibited transactions if they use the tools of the current legal framework. If the financial transaction uses traditional currencies, information about the funds and persons involved can be gathered, but cryptocurrencies enable anonymity. This means that funds for illegal activity can be transferred while the banking sector is incapable of responding to this. As a result, the financial institutions are relying more and more on technology that could potentially detect the legality of transactions that take place in a blockchain.[102] These types of legal efforts have been undertaken. For example, the Financial Action Task Force released a statement that there need to be efforts to prevent money laundering and funding of terrorism in virtual assets.[103] After this they adopted an interpretive note on new technologies.[104]

Cryptocurrency-specific regulation has not yet been adopted in the EU.[105] How governments deal with cryptocurrency covers a range of very different approaches, with some recognising it as a potential method of transaction and some not. The licence or authorisation given by a government can be a permit to operate in the entire EU area. In February 2018, Mario Draghi stated that there is a need to develop a single mechanism to ascertain the risks of funds or persons making transfers with cryptocurrencies. The idea is to bring cryptocurrency into the sector of traditional banking, where one knows one's customer in line with regular banking regulation.[106] The EU has argued that the current heterogeneous approach to cryptocurrencies enables illegal activity.[107]

Proportionality of sanctions concerning cryptocurrency is problematic. Cryptocurrencies are metaphorically coins with two sides. They have a positive effect and are part of the highest peak

[101] Fanusie, Y. (2018 October 11th) Seeking Sanctions Resistance Through Blockchain Technology, *Forbes*, 1
[102] Ibid.
[103] Financial Action Taskforce (FATF), "Public Statement – Mitigating Risks from Virtual Assets", February 22, 2019, https://www. fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets-interpretive-note.html.
[104] Financial Action Taskforce (FATF), "Public Statement on Virtual Assets and Related Providers", June 21, 2019, http://www.fatf-gafi.org/publications/fatfrecommendations/documents/public-statement-virtual-assets.html.v
[105] Houber, R. Snyers, A. (2018). Cyrptocurrencies and Blockchain: Legal Context and Implications for Financial Crime, Money Laundering and Tax Evasion, *European Parliament Study*, July 2018.
[106] Robinson, T. (2018 May 1) Inside Analysis on the Latest in Bitcoin, Ethereum & Blockchain, *Elliptic*.
[107] Binham, C. (2019 January 9) Cryptocurrencies: European Banking Authority calls for Pan-EU Rules on Crypto Assets", *Financial Times*,

in financial development in the world. On the other hand, they provide a method of moving criminal funds from person to person without detection. This is a difficult aspect when dealing with possible legal violations that involve cryptocurrencies. Freezing assets and travel bans are of course viable methods of EU intervention if there is strong evidence that cryptocurrency funds being transferred into the Union are meant for criminal operations, for example. But strong evidence might be difficult to collect, and the author suggests that dealing with cryptocurrencies as if they were all inherently suspicious is not in the interest of the Union. Cryptocurrencies pose a difficult task for the Toolbox, and a proportionate way of dealing with it is likely to bring challenges.

Dealing with cybersecurity incidents is rarely aimed at or limited to a specific market or nation since they spread to many regions. This makes the entire problem an international concern. Cybercriminal activities are specifically technological and are not involved with state politics or actions and are therefore likely to spread to multiple jurisdictions. In reality, cyberattacks that target one nation can have an impact outside that nation. The UN GGE has released a statement that there should be more co-operation between nations and organization on cyber incidents. In order to accelerate the use of safety measures, for instance, it is important to develop a global community of internet response teams or a global computer emergency response team. The global network of CSIRT systems or SOS system is an international effort to take responsibility for aiding the victims of an attack even when it is unknown who the attacker is. CSIRTs operate in co-operation with other CSIRTs to exchange best practices and information and lessons learned regarding the incident. CSIRTs do not have formal agreements between them, but their collaboration is based on trust and previous collaboration and on the assumption that collaboration benefits all parties. When an attack takes place, the CSIRTs exchange information on the nature of the attack and past experience of what has been the most effective way of tackling such a threat.[108]

[108] Pawlak, P. Biersteker, T. (2019). *Supra nota* 39, 84

5.2 The EU Cyber Diplomacy Toolbox in Action

This chapter focuses on the application of the EU Cyber Diplomacy Toolbox. The description of its use, targets, and features is based on the Council Decision (CSFP) 2020/1127 releases of the Council and related materials from the same official source.

The Cyber Diplomacy Toolbox has not remained idle since its release. During the summer of 2020 on July 30th, the Council announced that the sanction regime had been used for the first time. It emphasised that the Toolbox was created for a purpose and has been introduced into the field of cybersecurity. The release targeted six natural persons and three legal persons or entities. The sanctions in full effect, and the persons targeted by the regime have been prohibited from entering the Union's area, their assets have been frozen, and the EU also released a ban on supporting the individuals or entities financially. The reasons for their targeting were for a wide range of different attacks and malicious programs that had an effect on the EU. The attacks had a multitude of purposes ranging from financial gain to the investigation of organizations involved with international law. One of the attacks was an operation named "Cloud Hopper" that was traced to China, for which two people were sanctioned. The Cloud Hopper operation had a business interest, the aim of which was to collect sensitive financial data from companies and which had a significant financial impact on the companies. The attack itself was spread over six continents, but the sanction regime has effect only in the EU. [109]

The second larger attack was traced to the GRU. This attack was not named, but the target was the OPCW. The intention was to attack and get into the Wi-Fi network of the organization and collect intelligence regarding their recent investigations. The attackers got access to the network and were able to breach the Wi-Fi network, but the CSIRT of the Netherlands was able to intervene and prevent the cyberattack from doing more extensive damage to the OPCW's systems or investigations.[110]

The three entities targeted along with the individuals were partly commercial companies and partly governmental agencies. A company in Tianjin, China, named Haitai Technology Development Co. Ltd. was the main actor behind the Cloud Hopper operation. The two

[109] Council Decision (CSFP) 2020/1127 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, ANNEX A, natural persons 1, 2.
[110] Council Decision (CSFP) 2020/1127 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, ANNEX A, natural persons 3, 4, 5, 6.

individuals who were sanctioned were both linked to the company. The attack itself was conducted mainly by a person or persons known as APT10, who had links to the sanctioned individuals and the company. Therefore, the EU was able to determine a link between the natural persons and the company involved in the operation Cloud Hopper. No specific information was made public as to how the attack was conducted and what resources were used, but the fact remains that the sanctions were imposed on the company because it was heavily involved with the persons who were determined to be behind the attack.[111]

Chosun Expo, a Korean company, was also in the list of sanctioned companies. Their cyber operations were done under the name of WannaCry, which was examined previously in terms of its effects. Nevertheless, a link between the malicious program and the company was established, and the company has therefore been sanctioned for conducting the attack. The known perpetrators of the attack were APT38 or Lazarus Group, and their activity could be tied to the activity of Chosun Expo, which was therefore sanctioned. The internet aliases were connected with the perpetrators, and accounts of Chosun Expo were used to conduct the attack.[112]

The third sanctioned entity was the GRU from Russia. Even though individuals from the GRU were sanctioned, the GRU itself was not sanctioned for the OPCW attacks but rather for the NotPetya or EternalPetya attacks. An actor known as Sandworm played an active role in the NotPetya attacks against the Ukraine, disrupting that country's power grid and attacking companies in the EU. It has been established that the GRU played an active role in the activities of Sandworm.[113]

The application of the Diplomacy Toolbox was not the first response to these attacks. They had already been sanctioned by the United States sanction regime, and the attribution had been made in other countries as well.[114] In this case, the Diplomacy Toolbox did not bring any novel changes into the field of combatting malicious cyber operations and only established the same policies in the EU. Since it was a new sanction regime, there may have been hopes of it being

[111] Council Decision (CSFP) 2020/1127 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, ANNEX B, legal persons, entities and bodies, 1.
[112] Council Decision (CSFP) 2020/1127 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, ANNEX B, legal persons, entities and bodies, 2.
[113] Council Decision (CSFP) 2020/1127 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, ANNEX B, legal persons, entities and bodies 3.
[114] Department of Justice, The United States, Office of Public Affairs, "Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace" Retrieved: https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and Accessed: 19.12.2020.

deployed as a sort of pioneer in the field to target new finds. However, in the opinion of the author, this is an unimportant matter regarding the Toolbox and its initial steps. The fact that the Toolbox has already been applied is the most important thing in terms of its future use. The current sanctions will create non-theoretical consequences to the Toolbox and will show how the regime works in terms of the goals that have been set. Also, it shows how effective it is in terms of maintaining the sanctions so that keeping track of the individuals carrying out the malicious activity is organized in a manner that the sanctions are not mere declarations but their legal force is reliable in the Union's area. In the future we will also be able to see the results of the use of the Toolbox regarding the maintenance of travel bans and asset freezes, in addition to how the procedure of de-listing is handled in case there is sufficient reason for it.

From a strictly legal standpoint, the sanctioning of especially organizations can be justified in a number of ways. When an organization carries out an attack in another state, this potentially demonstrates shortcomings in terms of international responsibility on the part of the state from which the attack comes.[115] It means that this state did not exercise due diligence was not conducted properly since, as previously explained, a state should be aware of cyber activity coming from its territory to the degree that it can assess whether malicious operations are taking place. In the cases described above involving Korea, China, and Russia, due diligence had not been exercised. Granted, if there is state involvement in such an operation, it is obvious that due diligence has been neglected, but from a legal standpoint regarding international obligations, this principle has not been followed. However the case may be, the attacks were traced to these countries' territories so even if there is no possibility of direct attribution, there is clearly a possibility of indirect attribution.

In terms of proportionality, the sanctions seem quite reasonable since the responsible individuals were sanctioned and based on evidence backing the attribution to them. In terms of the sanctioned organizations, the involvement found was quite high, so that it did not seem like it was a single company worker carrying out the attacks and instead knowledge of the activity was more widespread in the company. In the case of the GRU, the organization was found to be active in the OPCW attack.[116]

[115] Chircop, L. (2018). A Due Diligence Standard of Attribution in Cyberspace, *International & Comparative Law Quarterly*, 67(3)
[116] Council Decision (CSFP) 2020/1127 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, ANNEX B.

Additionally, addressing the point of correct action under international law, the method used as the measure to the attacks was sanctions which would allow collective action, meaning the EU can apply these as a Union. The attacks that were attributed to the listed actors were quite damaging in the EU and posed a serious threat to the security of companies and impacted their financial standings. Whether the EU nations could carry out countermeasures is an interesting question. There would have to be strong evidence for attribution, which the author believes there is, which brings up the question whether the Toolbox a sufficient instrument for responding to these types of cyberattacks. WannaCry and NotPetya both had a large impact and to sanction individuals and organizations[117] with travel bans and asset freezes might not be the strongest approach to the situation. In terms of signaling, the Toolbox's application does serve a point and strengthens the deterring momentum the Toolbox has begun to develop.

[117] Council Decision (CSFP) 2020/1127 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, ANNEX A, B.

5.3 Future application of the EU Cyber Diplomacy Toolbox

The Toolbox represents a new step towards enforcing responsible activity in cyberspace. The Council decisions formulate the general framework for the system of sanctions that the EU is currently working to implement. The Council Regulation and Decision delineate the decision to create a sanction regime for cyberspace. Recital 7 makes it clear that the new Toolbox is intended to have a deterrent effect on cyber threats and to be capable of responding clearly to a particular threat.[118] The problem with these types of sanctions and measures is that as previously discussed the financial sanctions are not that impactful when it comes to coercing behavior.

The main point is to create specific sanctioning possibilities for the EU when encountering threats but also to work as a deterrent towards unfriendly intentions from third countries. The cyber diplomacy toolbox is not focused on a large-scale approach but has the approach to sanction individuals that are deemed likely to have conducted the attack. This is done in order to prevent a larger conflict from occurring between nations and limit the sanctions to individuals, the lowest level of sanction that there is.[120]

The approach in the Toolbox is reasonable since it does leave the decision of attribution to the Member States as well, so it does not want to provoke a larger conflict without their consent. However, the Toolbox does not specify which individuals or groups it can target. This ultimately leaves the door open for a larger political conflict to occur nevertheless because a state might be very inclined to keeping certain politically, financially, or otherwise influential persons protected and the Toolbox does have the possibility of stirring up a hornets' nest. This might not be likely, but although the Toolbox only targets individuals conducting attacks, this can become a state-level conflict because attacks by individuals are sometimes also organised or authorised by states. Sanctions might have bigger consequences than intended if the state is very supportive of the sanctioned group or individual. So even though the Toolbox aims to target only individuals, the individuals might be a part of something bigger and therefore a larger scale political conflict could occur. This is not an argument against the Toolbox nor to say that this is going to happen with certainty, but it is a risk that is not emphasized in the recent application of the Toolbox.

[118] COUNCIL DECISION (CFSP) 2019/797of 17 May 2019, concerning restrictive measures against cyber-attacks threatening the Union or its Member States
[120] Pawlak, P. Biersteker, T. (2019). *Supra nota* 39, 87

The problem that occurs with these types of sanctions and measures is that as previously discussed the financial sanctions are not that impactful when it comes to coercing behavior. The problem is that massive impacts could be caused by these types of sanctions, sort of contrary to the previous point, but it still is a potential mishap. An example of this is the very recent ban of WeChat, owned by the tech giant Tencent, imposed by the United States under the orders of President Trump.. The company had released a game called PlayerUnknown's Battlegrounds, which ranked 10th in the US consumer spend list in 2019.[121] The ban is part of the political conflict between the United States and China, but this example shows that if the Toolbox was to be used against a company such as Tencent or another major influence on the market for similarly reasons, it could have equally impactful effects on the single market. Whether the toolbox would be used in such scenario will remain to be seen but there is still the point that it could target a company that has a major impact on a single Member State and therefore the Toolbox does have greater power than initially displayed.

There is an interesting aspect to the Toolbox in the sense that even though it is a diplomatic measure, there seems to be not that much consideration regarding the diplomacy of using the Toolbox. The travel bans and asset freezes could go under a completely different scrutiny in addition to evidence based since the consequences of its application have a diplomatic or political nature. Therefore, the combatting of cybercrime would seem a bit different than what is clearly visible in the Regulation and Decision since a sanction regime that can apply to international actors can be more political and diplomatic and less evidence-based than in its earlier evaluations, and the state attribution only adds more variables to the process. Whether it becomes a diplomatic tool for diplomatic reasons or a tool for merely combatting cybercrime remains to be seen, but there are still strong political interests that go along with the decisions made.

[121] Pham, S. (2020 August 12) Tencent's profits are soaring. But it still has to contend with Trump's WeChat ban, *CNN Business*

The fundamental idea of the cyber sanction regime is that it provides strong deterrence and effective functions in practice. 'Building strong cybersecurity for the EU' of 13 September 2017 states that 'effective deterrence means putting in place a framework of measures that are both credible and dissuasive for would-be cyber criminals and attackers'.[122] The idea is to increase the legal forensic abilities so that legislation can be better enforced in cyberspace. Increased co-operation between the public and private sectors could be more effective in catching malicious activity in cyberspace. The deterrence of present cyber sanctions is rather vague and weak by reputation. The question is whether cyber deterrence and sanctioning can be created that have a stronger effect. The elusive or idealistic concept of EU sanctions is difficult to measure or point out, which leads to unmet goals. In order for the cyber sanction regime to have a deterrent effect, it is necessary to develop concrete political instruments. [123]

Solidarity and defense clauses exist mainly as deterrents to traditional military threats. Such clauses have not yet been interpreted to prevent and deal with cyber threats because this field has developed rapidly quite recently. Such clauses are nevertheless well applicable to cyberspace and create a framework on the basis of which the EU can improve the Toolbox to be more effective and sophisticated in preventing and dealing with cyber threats.

Since Member States deal with cyber threats differently and since their capabilities are also quite different, it is natural that they also have different opinions. The idealistic approach of the previous paragraph of moving forward in solidarity with a joint strategy on cyber threats is not a likely step to be taken, or if it is, the process will be quite slow. The Toolbox might create an EU-based approach to targeting malicious cyber actors so that attribution at the state level would decline and the EU could take the lead if the co-operative approach would be too arduous to maintain.

The EU sanctions consist of two different measures: travel bans and asset freezes. These can be targeted towards legal or natural persons.[124] The sanctions need to be proportional, and it should be considered whether the sanctions have more extensive consequences than intended. In many cases, there is some governmental involvement in cyberattacks, and therefore consideration is needed regarding sanctions affecting governmental behavior.

---

[122] European Commission, Joint Communication to the European Parliament and the Council, *"*Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU*", JOIN (2017) 450 final*, Brussels, September 13, 2017.
[123] Pawlak, P. Biersteker, T. (2019). *Supra nota* 39, 89
[124]COUNCIL DECISION (CFSP) 2019/797 of 17 May 2019, concerning restrictive measures against cyber-attacks threatening the Union or its Member States

The duration and dates of cyber sanctions have a strong influence on how effective they are. They are designed to be flexible, and they can be adapted as the situation changes, which suits cyberspace very well since the environment and discovered facts can change greatly in a short time. Council Decision 2019/797 requires the renewal of sanctions if the goals set have not yet been met. The Council Regulation allows, in the Annex I, for the listing to be expanded or altered based on new information. The list needs to be renewed after a certain time intervals or at least annually. These features are extremely important when the actor behind the malicious cyber activity is being tracked down. [125] The first listing took place in July 2020, and there is no experience yet on the actual flexibility of the listing and delisting process.

It is interesting to see how the potential delisting due to changing circumstances will work if it is ever done. The question of how long the sanctions are held in place and assets are frozen will be something for the future. The first use of the Toolbox in July 2020 has shown that there are a few persons known to whom the Toolbox has been applied. Judging by the information about those cases, it seems unlikely that there will be delisting based on false targeting, however it is not impossible. Another interesting aspect regarding the future is that Chosun Expo seems to be a long-dormant Korean and Chinese joint venture, and both governments deny any kind of link to the company. News stories seem to be skeptical that there are any assets that could be frozen.[126]

Another aspect of the Toolbox's conclusions is that they do not mention specific methods of evidence collection or procedures of listing individuals. Since these are not transparent because they might include sensitive information which if exposed could damage the whole spectrum of trust and trade between the EU and third countries. In the first listing done in July 2020, the EU did not release information about the process but named the main suspected actors and their connections to the attacks, as covered in the chapter of the Toolbox's first application. It does have the element of being used as a political tool if the reasons are not transparent and therefore the travel bans and asset freezes could be imposed on a slightly less convincing evidentiary basis on a person who is a persona non grata in the Union. This would create a new aspect of being a political tool to the mix and this essentially might not be in the interest of the Union in the long run, but it is not impossible to use for these and other purposes. The aspects of a cyberattack or crime are widely accepted to be very difficult to clarify and bring clear evidence of, so this

[125] Pawlak, P. Biersteker, T. (2019). *Supra nota* 39, 92
[126] Kasulis, K. (2020, July 22). European Union to impose cyber sanctions on North Korea due to cyberattacks, *North Korea News*

element can go both ways and make it an easier to use tool which can be used as a different type of tool than for threat control.

Another key aspect is the time spent while making the decision to list someone. The decisions to set up, add to, or publish a list are mentioned in the Annex, and these decisions need to be proposed by a Member State and need to be made unanimously by the Council.[127] Considering the sensitivity of the topic, it is unlikely that these decisions are made quickly or without warning the target. This makes it likely that the target can prepare for alternate approaches to counter the decisions' effects.[128] The preparation of the listing in the first application took somewhat longer since the perpetrators were known and already listed in the United States.[129] Whether it is a question of the length in procedure or simply of the fact that the Toolbox is completely new is uncertain, but perhaps a mix of both.

The effectiveness of the application of the Toolbox will be seen in practice. Since it is based on sanctioning, it is retroactive and cannot function in the forefront of dealing with cyber threats. Developing the effectiveness of MLAT co-operation[130] is important along with the EU's own intelligence gathering to shorten the time between the cybercrime and sanctions. The pace at which the sanctions can be applied is extremely important to have the Toolbox be a relevant legal instrument. If the application of sanctions is shown to be effective and very engaged in the field of cyber threats, the deterrence effect can be improved. Improvement of the Toolbox's deterrence effect will be something that the EU can be successful in or not. If the Toolbox has an impact on cyber actors so that there is an actual threat of being listed for malicious activity, the Toolbox can have a strong impact regardless of the fact that it is based on low-level sanctioning. The greater impact that the deterrence has, is that is always in applicable. The deterrence effect does not have to rely on actual sanctions to influence the field at all times.[131]

Given the circumstances for the decision making, it is quite likely that the impact of the sanctions is quite low. Since the mechanism of the decision making can take some time, alternate lower level methods like pursuing the criminals and bringing charges against them should be

[127] COUNCIL DECISION (CFSP) 2019/797of 17 May 2019, concerning restrictive measures against cyber-attacks threatening the Union or its Member States
[128] Pawlak, P. Biersteker, T. (2019). *Supra nota* 39, 92
[129] Department of Justice, The United States, Office of Public Affairs, "Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace" Retrieved: https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and Accessed: 19.12.2020.
[130] Pawlak, P. Biersteker, T. (2019). *Supra nota* 39, 80
[131] Ibid., 88

considered. The question is whether it is more effective to pursue these criminals with police forces and court proceedings or to have them listed and sanctioned.

When applying sanctions, it needs to be considered how they are applicable together with other instruments like the legislation of a given country. It complicates the process in the sense that there needs to be a mutual understanding on what is done with a cyber threat in terms of the diplomatic toolbox and the independent court systems of the Member States. When there is focus on individuals or entities, the EU has admitted that individuals or non-governmental actors, like state proxies, can cause a grave threat to EU security.[132] This is mainly because the individuals have been somehow linked to governments or have received some level of support. At the same time, the sectoral sanctions or country specific sanctions are absent, which is probably due to the EU trying not to cause too much political turmoil in the sanctioning process. This approach is beneficial in the sense that the sectoral approach could lead to political conflicts or escalation of existing tension, both of which are in the interest of the EU to avoid. This is why it is important to maintain discussion and have processes in place that can lower the tension and ultimately calm political conflicts. The Council Decision entails the exception that if someone is placed under a travel ban, they still are allowed to travel to inter-governmentally arranged meetings if the topic of the meetings is cyberspace and security. Focusing on the OSCE is important since it is one of the few places where discussions between the EU and Russia can take place.[133]

There is still time to increase the understanding of potential targets and decrease the likelihood of escalation of conflicts, for example by following the rules of the NIS Directive. When political proposals are difficult to discuss with Russia or China, it is important to arrange meetings at the level of experts, where political efforts are ineffective.[134]

A vast amount of expertise is needed to impose sanctions and have them followed through. It is extremely important to maintain and adapt them due to the fast pace of developments in cyberspace. The cyber diplomacy toolbox's sanction regime gives the EU a new tool to operate with. It requires a lot of work and takes up a lot of resources, while there are no targeted funds for these processes carried out by the EEAS.[135] The threat to the cyberattacks there is no possibility to invest in the matter as the public discourse would promote to be necessary. This leads to different Member States having different capacities to approach these problems on their

[132] Pawlak, P. Biersteker, T. (2019). *Supra nota* 39, 93
[133] Ibid., 94
[134] Ibid., 94
[135] Ibid., 95

own, which can mean that the cyber sanctioning regime has different results in different countries. Nowadays only a few countries have the capacity to deal with cyberattacks, including the UK, the Netherlands, France, and Estonia. The Member States have to trust the information that they receive from the public sector or from bilateral co-operation. The culture of information sharing needs to be strengthened to develop these capacities.[136]

Private sector actors are creating norms, and this creates questions regarding their legitimate enforcement. Private sector actors are mostly interested in producing profit, which is not necessarily in the interest of a government. When they are involved in discussions of cyber security, they are mostly American or European companies, which makes it questionable how global the initiatives are. The question is extremely important when it comes to attribution that has significant effects on governmental relations and countless companies in the EU and third countries.[137]

[136] Pawlak, P. Biersteker, T. (2019). *Supra nota* 39, 95
[137] Pawlak, P. Biersteker, T. (2019). *Supra nota* 39, 98

6. CONCLUSIONS

The internet has provided the market, communication and governmental services, and other endeavors with great possibilities to expand and become more efficient and widespread. The internet has not developed without a darker side. Internet crime has been a part of the web for a long time and is easily conducted by smaller groups or even individuals. Solutions on the technological side combat this crime, but solutions cannot be provided only on the commercial and technological side. The EU has united its forces in an effort to develop a diplomatic tool for combatting crime originating from third countries and combatting malicious governmental activity coming from outside the EU. The Council Decision 2019/797 and Regulation 2019/796 creating the Cyber Diplomacy Toolbox are the EU's latest developments taking the initiative to combat cybercrime, which can be seen as a culmination of UN statements, prior EU statements, and other nearly global efforts to somehow regulate cyberspace. The main ideas derived from the EU's activities are that identified perpetrators can be prohibited from entering the EU and that their assets they in the EU can be frozen.

Financial sanctions are, in the case of the Toolbox, the freezing of assets, even though travel bans might have financial consequences for individuals. The sanctions themselves are not very useful for achieving a goal, as the research done on UN sanctions shows. The studied effectivity of sanctions and the success percentages were quite low across the board. The utility of sanctions is most visible when they are part of a larger operation as a subsidiary tool, but not as the main approach. In some cases, sanctions have had large impacts, for example the economic sanctions imposed by the United States on Nicaragua. Additionally, the future will show how the Tencent situation develops if the decisions to limit their access to the market in the United States is affected. But an essential deficiency in the Toolbox is that sanctions are not statistically deemed an effective approach to deal with a situation and require the addition of other efforts in order to have a sufficient signaling or coercing effect on a person, group, or organization. The Toolbox's sanctions are also slightly flimsy in terms of travel bans being approved or prohibited by nationally competent authorities. Even though the EU can prevent a decision made by a Member

State to permit transit, the correspondence between the Union and the Member State might not be quick enough in practice to actually enforce a travel ban on an individual with consistency.

This paper's comparison between international law and the Toolbox show that it conforms to international rules and norms. The commercial sector is involved in the matters regarding the use of toolbox, since the commercial sector possesses great amounts of capabilities and information on cyberspace. Their involvement in the diplomatic process of setting norms of behavior in cyberspace is however questionable.

The Diplomacy Toolbox conforms with international norms, and what follows is the inevitable application of proportionality in the procedures. The legal elements that are in consideration regarding the international use of the toolbox are the methods of use. Retorsion, countermeasures, and self-defence are the international methods of responding to hostile activity, and when they can be used depends on the severity of the situation, and joint use is limited as well. The Toolbox as legal instrument provides tools to engage in these situations in accordance with international law.

Attribution is one of the key elements in the application of the Toolbox, which provides criteria for its legitimate use. Attribution has been left as the decision of Member States, which causes especially efficiency and consistency problems in the application of the toolbox. The problem is made worse by the technological and legal differences in the Member States, which make a consistent joint response unlikely. Gathering intelligence in order to attribute an attack to persons or entities requires cooperation between Member States to share this information, which is not yet the norm between Member States. The intelligence can also include information considered sensitive information by a state, which would further deter that state from sharing it with other governments or in public notices or statements. An environment where Member States could share this information is still far ahead and requires other steps to be taken in order to be achieved.

Due diligence is required of states in order to attribute attacks but also to fulfil their responsibilities regarding international law. In essence it means that a state needs to be aware of the kind of cyber activity that is taking place within its territory and infrastructure. In principle the concept is quite clear, but in practice a state’s ability to fulfil their duties varies greatly and when reviewing proportionality, this is extremely important.

The private sector is involved in co-operation with the states or at least shares the interest to prevent cybercrime. This co-operation is quite efficient at the moment, and the private sector has

had initial responses to cyberattacks in protecting their assets. This shows how important the co-operation is, since most of the capabilities are in the private sector and developed there. The norm creation in the private sector can also be important when the future of cyber security is shaped.

Cyber sanctions are not completely straightforward; they of course have their intended goals but there are unfortunately also unwanted or unpredictable consequences. Analyzing the proportionality of sanctions is very important since it is reasonable to analyze whether certain actions create more harm than benefit. The Toolbox has not yet been modified to solve the problems that might arise as side effects.

Cryptocurrencies have taken the internet by storm and are more and more in use. This has not happened without problems since they are anonymous in their nature and make the tracking of criminal activity more and more difficult. They have a lot of benefits like the blockchain technology, but states are not yet able to prevent them from being used for criminal purposes. It is extremely demanding, but states need to be more involved in the activities of these technologies in their cyberspace.

The use of the diplomacy toolbox has the effect of punishing cyber criminals but also that of the threat of punishment creating deterrence against cybercrime. Due to the novelty of the diplomacy toolbox, it is too early to evaluate how its deterrence works. In the past, however, deterrence has not been the most effective method against cybercrime. The first application of the Toolbox has shown that it is in use and that the mechanisms are applied, but not much data has yet been collected in the aftermath of the Toolbox's first application.

The Toolbox is an ambitious effort to create a legal order in cyberspace using a model of sanctioning as a response to cyber attacks. There is some doubt regarding its efficiency in cyberspace in coercing legal behavior or deterring cybercrime since earlier studies on sanctions have shown that they are not alone sufficient. As evidence starts to accumulate about the practical effects of the Toolbox's first application in July 2020, this will indicate whether the Toolbox needs some altering to serve the purpose it has been created for or not. The toolbox in its core is not completely novel because the methods it uses are traditional methods in diplomacy, but their application in cyberspace is cutting edge. It seems likely that it is necessary to further develop the scope, efficiency, and swiftness of the Toolbox.

In general, in accordance with the Council Decision the Toolbox applies to persons that are located outside Union, and to attacks that are carried out and originate, outside the Union. The

stated scope of the attacks consists of access to information systems, interference with information systems, data interference and data interception. These attacks can target critical infrastructure in all its forms, structures maintaining essential services for social or economic activities and critical functions like state defense. Thus, the stated scope of the Toolbox is far reaching. However, the sanctions of the Toolbox target individuals and legal persons meaning the actual scope of the Toolbox is quite narrow. The targeted cyber activity is extremely wide but in case of sanctions the scope does not reach the same level.

The legal implications of the Toolbox are proportional and quite straightforward. However, that is not to say that the Toolbox and its measures are sufficient against malicious cyber operations. The Toolbox still has the potential of deterring criminals from carrying out cybercrimes and sanctioning the criminals if they have participated in the crimes. Unfortunately, malicious cyber operations are still increasing in number, and it would be reasonable to assume that states are going to carry out more cyberoperations against each other.

The sanctions of the Toolbox target individuals and entities meaning that the actual scope of the sanctions is quite narrow. However, the activity within the scope threatening cyber activity it still has the potential of deterring criminals from acting out these operations and sanctioning them if they have been participant to such operations. The unfortunate fact is that the malicious cyber operations are still a growing field and it would be reasonable to assume that states are going to be more active in the field against each other. Looking at the actual scope from this perspective it is extremely narrow. In case there is going to be continuously more and more state involvement in cyberattacks punishing the individuals with the sanctions of the Toolbox is nowhere near sufficient.

In terms of international law, the sanctions should be proportionate. The official EU statements and regulations considering the Toolbox do not directly mention the principle of proportionality, but since the Toolbox operates in the field of international law, one can assume that it is designed to follow the principle. In the first instance where the Toolbox was applied, the principle of proportionality was clearly followed. But looking at the growing trend of state involvement in cyber operations, there would have to be a more unified and powerful tool or alteration to the Toolbox in order to create a more effective sanctioning regime. If that is the direction in which this field develops, the principle of proportionality will likely become more difficult to fulfil.

List of References

Books

1. Craig, P. de Burca G. (2011). *EU LAW, Text, Cases and Materials*. (5th ed.) New York. Oxford University Press.
2. Hufbauer G. *et al*., (2007). *Economic Sanctions Reconsidered,* Washington DC. Peterson Institute for International Economics
3. Schmitt, M. (2013). *Tallinn Manual on The International Law Applicable to Cyber Warfare*. Cambridge University Press.
4. Schmitt, M. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press.

Journal Articles

5. Allan, C. S. (2013). Attribution issues in cyberspace. *Chicago-Kent Journal of International and Comparative Law,* Vol. *13*(2*)*, 55-83.
6. Anderson, T. (2017). Fitting virtual peg into round hole: Why existing international law fails to govern cyber reprisals. *Arizona Journal of International and Comparative Law*, Vol. 34(1), 135-158.
7. Biersteker, T. Eckert, S. Tourinho M. Hudáková, Z. *The Effectiveness of United Nations Targeted Sanctions: Findings from the Targeted Sanctions Consortium (TSC)* (Geneva: Graduate Institute of International and Development Studies, 2013). 1-51, 21-23.
8. Boeke, S. National cyber crisis management: Different European approaches, *Governance, an international journal of policy*, administrations and institutions, 31(3), 449-464.
9. Carrapicco, H. Barrinha, A. (2017). The EU as a Coherent (Cyber)Security Actor? Journal of Common Market Studies, 55(6) 1254-1272.
10. Chircop, L. (2018). A Due Diligence Standard of Attribution in Cyberspace, *International & Comparative Law Quarterly*, 67(3)
11. Doxey, M. (1972). A framework of Analysis with Special Reference to the UN and Southern Africa, International Organization, 26(3), 527-550.
12. Dupont, P. (2012). Countermeasures and Collective Security: The Case of the EU Sanctions Against Iran", *Journal of Conflict & Security Law*, 17(3), 301-336.

13. Eichensehr, K. (2017). Public-private cybersecurity. *Texas Law Review*, 95(3), 467-538.
14. Gary C. Hufbauer G *et al*., (2007). *Economic Sanctions Reconsidered*, Washington, DC: Peterson Institute for International Economics.
15. Gurkaynak, G. Yilmaz, I. Taskiran, N. (2013). Governmental Efforts and Strategies to Reinforce Security in Cyberspace, *International Law Research*, 2(1), 185-194.
16. Henderson, J. (1986). Legality of economic sanctions under international law: The case of Nicaragua. *Washington and Lee Law Review*, 43(1), 167-196.
17. Higbee, A. (2018). The Role of Cryptocurrency in Cybercrime, *Computer Fraud & Security*, Issue 7, 13-15.
18. Lin, H. (2012). Dynamics and Conflict Termination in Cyberspace, Strategic Studies Quarterly, 6(3) 46-70.
19. Lindsay, J. (1986). Trade Sanctions as Policy Instruments, *International Studies Quarterly*, 30(2) 153-173.
20. Leogrande W. (1996). Making the economy scream: Us economic sanctions against Sandinista Nicaragua, Third World Quarterly.
21. Mejia, Eric F. "Act and Actor Attribution in Cyberspace: A Proposed Analytic Framework." *Strategic Studies Quarterly*, 8 (1), 2014, 114–132.
22. Moret, E. Pothier, F. (2018). Sanctions After Brexit, *Survival: Global Politics and Strategy*, 60(2), 179-200.
23. Mudrinich, E. M. (2012). Cyber 3.0: The Department of Defense Strategy for Operating in Cyberspace and the Attribution Problem. *Air Force Law Review*, *68,* 167-206.
24. Osula, A. (2015). Mutual Legal Assistance & Other Mechanisms for Accessing Extra Territorially Located Data. *Masaryk University Journal of Law*, 9(1), 43-64 46-50.
25. Reddy, E. Minnaar, A. (2018). CRYPTOCURRENCY: A TOOL AND TARGET FOR CYBERCRIME, *Acta Criminologica: Southern African Journal of Criminology,* 31(3), 71-92.
26. Roscini, M. (2014). *Cyber Operations and the Use of Force in International Law* (Oxford: Oxford University Press)
27. Ryan, D. *et al*. (2011). International cyberlaw: normative approach, *Georgetown Journal of International Law*, 42(4), 1161-1198

28. Schmitt, M. (2014). Below the threshold cyber operations: The countermeasures response option and international law. *Virginia Journal of International Law*, 54(3), 697-732.
29. Schmitt, M. (2015-2016). In Defense of Due Diligence in Cyberspace. *Yale Law Journal Forum*, 125, 68-81.
30. Shamsi, J. et al. (2016). Attribution in cyberspace: techniques and legal implications, *Security and Communications Network*, 9(15), 2886-2900.
31. Shackelford, S. J., & Andres, R. B. (2011). State responsibility for cyber attacks: Competing standards for growing problem. *Georgetown Journal of International Law*, 42(4), 971-1016.
32. Tikk, E. (2018). Will Cyber Consequences Deepen Disagreement on International Law, *Temple International & Comparative Law Journal, 3*2(2),185-196.
33. Turner, A. et al. (2019). A target-centric intelligence approach to WannaCry 2.0, *Journal of Money Laundering*, 646-665.

News Articles

34. Binham, C. (2019 January 9) Cryptocurrencies: European Banking Authority calls for Pan-EU Rules on Crypto Assets", *Financial Times*.
35. Fanusie, Y. (2018 October 11th) Seeking Sanctions Resistance Through Blockchain Technology, *Forbes.*
36. Kasulis, K. (2020, July 22). European Union to impose cyber sanctions on North Korea due to cyberattacks, *North Korea News.*
37. Laurens, C. (2020, June 22) Von der Leyen calls out China for hitting hospitals with cyberattacks. *Politico*
38. Pham, S. (2020 August 12) Tencent's profits are soaring. But it still has to contend with Trump's WeChat ban, *CNN Business.*
39. Robinson, T. (2018 May 1) Inside Analysis on the Latest in Bitcoin, Ethereum & Blockchain, *Elliptic*.

European Union legislation

40. Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union
    2012/C 326/01, Article 36
41. Directive 2016/1148 of the European Parliament and the Council concerning measures for a high common level of security of network and information systems across the Union", Brussels, July 7, 2016.

Decisions, Communication and Council Regulation

42. COUNCIL DECISION (CFSP) 2020/1127 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States
43. Council of the European Union, Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox") Brussels, 7 June, 2017.
44. Council Decision 2019/797 considering restrictive measures against cyber/attacks threatening the Union or its Member States.
45. Council of the European Union, *Council Conclusions on Cyber Diplomacy*, Brussels, February 11, 2015.
46. European Commission, Joint Communication to the European Parliament and the Council, *"*Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU*"*, *JOIN(2017) 450 final*, Brussels, September 13, 2017.
47. Council Decision (CSFP) 2020/1127 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, July 30, 2020.
48. COUNCIL REGULATION (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States

Official publications

49. Bendiek, A. (2012). European Cyber Security Policy, SWP Research Paper No. 13
50. Botek, A. (2019). European Union establishes a sanction regime for cyber-attacks, INCYDER Database, The NATO Cooperative Cyber Defence Centre of Excellence. Retrieved: https://ccdcoe.org/library/publications/european-union-establishes-a-sanction-regime-for-cyber-attacks/ Accessed: 17.8.2020
51. Eggenschwiller, J. (2019). International Cybersecurity Norm Development: The Roles of States Post-2017", *Research in Focus, EU Cyber Direct*, March 2019, 1-11. 9
52. Department of Justice, The United States, Office of Public Affairs, "Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace" Retrieved: https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and Accessed: 19.12.2020.
53. Ivan, P. Responding to cyberattacks: Prospects for the EU Cyber Diplomacy Toolbox, *EPC Discussion paper*, 18 March 2019, 3-13.
54. Houber, R. Snyers, A. (2018). Cryptocurrencies and Blockchain: Legal Context and Implications for Financial Crime, Money Laundering and Tax Evasion, *European Parliament Study*, July 2018.
55. Pawlak, P. Biersteker, T. (2019). Guardian of the Galaxy, EU cyber sanctions and norms in cyberspace, *Chaillot Paper 155*, October 2019, European Institute of Security Studies, Paris, 1-103.
56. UN GGE: Efforts to Implement Norms of Responsible State Behaviour in Cyberspace, as Agreed in UN Group of Government Expert Reports of 2010, 2013 and 2015. Retrieved https://www.un.org/disarmament/wp-content/uploads/2019/12/efforts-implement-norms-uk-stakeholders-12419.pdf Accessed: 17.8.2020
57. United Nations General Assembly (UNGA), "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," July 22, A/70/174, 2015. 1-17.Wessel, R. (2015). Towards EU Cybersecurity Law: Regulating a New Policy Field, in Tsagourias, N. Buchan, R. (eds) Research Handbook on International Law and Cyber Space (Cheltenmham Edward Elgar Publishing) 403-425

Web materials

58. CyberPeace Institute, Case Study: WreckWeb. Dealing with Notpetya. Retrieved: https://cyberpeaceinstitute.org/assets/news-articles/wreckweb_single_page.pdf Accessed: 17.8.2020
59. Financial Action Taskforce (FATF), "Public Statement – Mitigating Risks from Virtual Assets", February 22, 2019, Retrieved: https://www. fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets-interpretive-note.html. Accessed: 16.10.2020
60. Kaspersky Threats, EMAIL-WORM.VBS.LOVELETTER, (200 May 5) https://threats.kaspersky.com/en/threat/Email-Worm.VBS.LoveLetter/ Accessed:16th October 2020.
61. Moret, E. (2015). "Humanitarian Impacts of Economic Sanctions on Iran and Syria", *European Security*, vol. 24: 1#

Graduation Thesis

62. Kivihuhta J. (2018). *Principle of Distinction in Cyber Operations*. (Bachelor's Thesis) Taltech School of Business and Governance Tallinn.
63. Tolppa, M. (2018). *Standard of Proof in Attribution of Internationally Wrongful Cyber Operations,* (Master's Thesis) Taltech School of Business and Governance Tallinn

Blog posts

64. Gail, K. (2015). The Mutual Legal Assistance Problem Explained, The Center for Internet and Society, Stanford Law School [Blog Post] Retrieved: http://cyberlaw.stanford.edu/blog/2015/02/mutual-legal-assistance-problem-explained Accessed: 12.8.2020
65. Romanosky, S. (2017). "Private-Sector Attribution of Cyber Attacks: A Growing Concern for the U.S. Government?", Lawfare, [Blog Post] December 21, 2017. Retrieved from: https://www.lawfareblog.com/private-sector-attribution-cyber-attacks-growing-concern-us-government, Accessed: 12.8.2020

Other

66. https://searchsecurity.techtarget.com/definition/cyber-attribution Definition: cyber attribution