The Importance of Regulating Cyberspace from the Perspective of International Law- Applications

Adrian MALDEȘ
Carol I National Defense University, Bucharest
adi_maldes@yahoo.com

Abstract: The increase in frequency and strength of cyber-attacks in the current period has led to meetings between NATO and EU allies and other organisations to address issues related to cybersecurity. Discussions focused on the adoption of regulations, a legal framework, or directives, in order to support allied states in the fight against cybercrime. The discussions included not just the drafting of a legal framework regarding cyber-attacks, but also the classification of cyber as an operational domain for the militaries, and the necessity to apply the provisions of Article 5 from the North Atlantic Treaty signed in Washington D.C. on the 4th of April 1949. The lack of an international legal framework raises a lot of challenges. This represents a challenge for the allies, the members and organisations, taking into consideration the fact that, at the last NATO Summit, new topics were brought into discussion, regarding the cooperation on cybercrime between allied states, the drafting of a Protocol V or the amendment of the Geneva Convention from 1949, and by introducing cybernetic warfare as a violation of international law. The article argues the necessity of drafting a Protocol V or an amendment to the Geneva Convention from 1949, which would state that cybercrime is a violation of international law. The context is a dire one, considering the fact that the allied states of NATO and the EU but also the UN in general cannot adequately manage and hinder cybernetic attacks, both from inside and outside of the state and mitigate their effects.
Keywords: Cybernetic Attacks, Cybernetic Space, Legislative Harmonisation, Regulations, International Law

INTRODUCTION

After the emergence of the Geneva Convention in 1949 and its protocols, both state and non-state actors followed and implemented the provisions of international law. However, starting in the late 20th century, another branch of warfare started to develop, whose operations took place in cyberspace and which presented significant differences compared to traditional hostile action.

The question of how war in cyberspace can be classified as a conflict is of paramount

importance and a coherent answer must be found as quickly as possible in order to repel the attacks (The European Commission, 2017). Some of the members of NATO, including the USA and the United Kingdom, have made intense efforts in order to develop their capabilities in what is described as cyber warfare. Not even the EU was left behind, and it seems that starting with 2013 there has been a strong emphasis placed on the field of cyber security (Ranger, S., 2014). It is obvious that, until now, the EU has tried and managed to make big steps in cyber security (Ministry of External Affairs, 2021).

Until the development of global regulations that would offer support both from a constructive point of view, but also from the point of view of fighting against security incidents, all organisations are confronted with a very serious problem, which is the lack of cooperation and trust between the public and private sectors which complicates the fight against cyber-attacks at the global level.

This situation can mainly be observed in the private sector. Due to the absence of trust in authorities, of financial support in case of cyberattacks, and because of other adverse incentives (cumbersome and time-consuming procedures), small and medium businesses usually prefer to pay ransom to hackers instead of resorting to other modes of resolution for cyberattacks. The pressure that is exerted on this type of entities transforms them into easy targets for cyberattacks, as their goal is to resume their normal workflow as fast as possible, no matter the costs(The European Court of Auditors, 2019).

Although the EU and the USA are making efforts to prevent cyber-attacks and the former has recommended to Member States to take the appropriate measures in the short and long term in order to defend against this type of attack, not all of the states have the possibility to advance at the same pace, which means, that at this moment, we cannot talk about organisations that are strong enough to prevent any cyber-attack.

In fact, global organisations are trying to consolidate cybernetic resilience as one of the main elements of security, both for NATO and the EU, reflected through "The Directive regarding the security of networks and information systems adopted in the year 2016" (Publication office of the European Union, 2018).

A recent stake for this consolidation is represented by the emergence in the mainstream of a new technology, 5G, that can create problems for a lot of states, especially those that are slow to implement or comply with the recommendations, directives and other relevant EU documents (The European Commission, 2019). Member States are under the obligation to adopt these in the national legislation, in order to support not just generic cybersecurity, but also the security of specific sectors such as energy, various industries, public administration and so on (The European Union Council, 2021).

Both in response to traditional crime, as well as to the rise in cybercrime and to the use of modern technologies in order to commit crime, the European Council comes with the proposition for new rules regarding electronic evidence. These rules regulate the access to electronic evidence in order to fight crimes in the digital era (The European Union Council, 2020b).

The new rules define the way in which Member States can request and keep electronic evidence, without the challenges of creating a new judiciary procedure.

Discussions are also taking place regarding the implementation of an agreement between the EU and the US in order to facilitate the transborder access to electronic evidence, in on-going criminal proceedings (The European Union Council, 2021).

This takes place in the context of massive investments on the part of states in developing cybernetic capabilities which have both civilian and military uses (The

European Commission, 2020) and which may then trickle down to proxy actors for hybrid warfare and to cyber criminals.

CYBERNETIC SPACE FROM A LAW PERSPECTIVE - A LEGISLATIVE HARMONY

In the last decade, there have been certain principles which regulated the evolution of legislation in the field of cybernetic security (The European Commission, 2020), which often took the form of conventions, non-binding declarations, memoranda and others. Starting with the year 2013, the EU started to support international or even global actions in order to manage cyber-attacks (The European Union Council, 2019a).

As part of the major involvement of the EU in the management of the attacks and of the disturbances that have appeared in this area, European Directive 1148/2016 was developed (The European Parliament and The European Union Council, 2016), which represents the foundation for the Union to shape and mandate Member States to implement and take actions/decisions in order to combat cyber-attacks (The European Commission, 2020).

Following the analysis made by the European Court from 2019, and together with the constructive support of other organisations, like the European External Action Service, ENISA, Europol, the European Organisation for Cybernetic Security, it has been concluded that, starting with the year 2013, cybernetic attacks have rapidly evolved affecting governments, which made the ultimate financial and budgetary impact much higher today than in the year 2013 (The European Court of Auditors, 2019).

Together with the entry into force of the Budapest Convention on Cybercrime (2001, entering 2004), the EU took tougher measures regarding the fight against cyber-attacks through the adoption of new directives, the establishment of new organizations, rules, legal frameworks (establishing ENISA, Framework Decision regarding cyberattacks, establishing CERT-EU, Directive regarding cyberattacks) which aim to support the prevention of cyber-attacks (The European Union Council, 2004).

The momentum of the European Union manifests itself partly through the large number of meetings and conventions between member states in the European Council starting with the year 2017. After these meetings, the conclusions of the Commission were in the direction of common communication and the completion of cybernetic security packages. Therefore, the Commission considered that it is highly necessary that the security packages contain important elements, necessary to repel cybernetic attacks, which were categorized as resilience, discouragement and defence against attacks (The European Commission, 2013).

In later years, the EU has updated the cybernetic security package, with a proposal for the so-called Network and Information Security (NIS) Directive being updated in December 2020, and encompassing a host of new developments (The European Parliament, 2021).

At the NATO, EU and UN level, a multitude of institutionalised types of temporary or permanent mechanisms have been developed in the form of programs that aims to stop cybernetic attacks, and to find in the shortest amount of time a way to quickly and durably develop computer systems that can resist these attacks (The European Union Council, 2019b).

The EU always underlined the major importance that cyber security regulations at European (therefore collective) level have on resilience, on sovereignty and on the protection of people, companies and institutions against cyber-attacks. Moreover, the Council of the European Union is waiting for a fast application of the Regulation in the subject of Cyber Security and the operationalisation of Cybersecurity Competence Centre in Bucharest (The European Union Council, 2021). As such, it

is important to notice the increase in the number of regulations and policies along the years in the EU, in order to keep up with the ever increasing cybersecurity threats (Fig. 1).

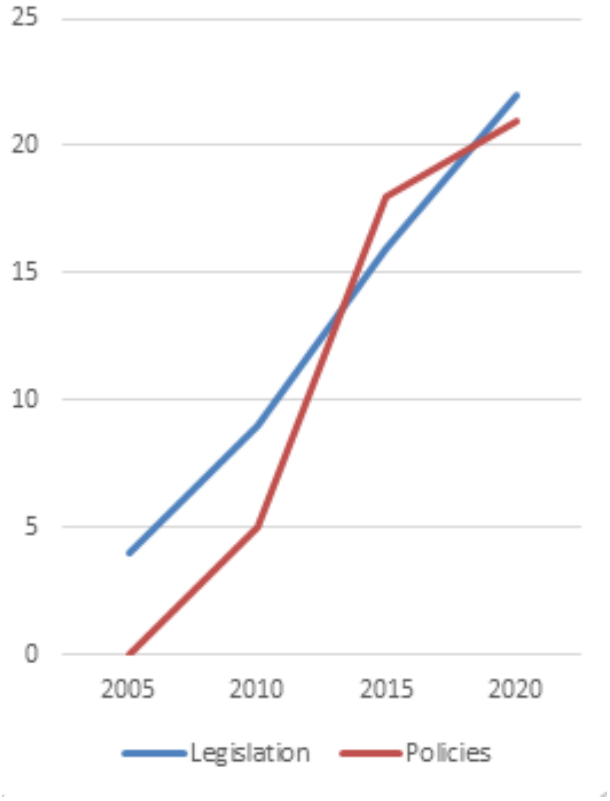

Fig. 1: *The increase in the legislative and policy elaboration process regarding cyber-security in the EU*

CYBER ATTACKS TAKING INTO CONSIDERATION THREAT EVOLUTION AND THE NECESSITY OF APPLICABLE INTERNATIONAL LAW

In the last 30 years, communication and information technologies developed at a very fast pace. Although the specialty literature mentions the 11th of September as a starting point for a new age of warfare, it has become obvious that the cybernetic world has big vulnerabilities that have been superficially treated in the past. The key incidents that provided wake-up calls were the 2007 attacks in Estonia, followed closely by the incidents from the year 2008.

2008 is the year that practically proved that a cybernetic attack can be costly for states because of the vulnerabilities that were present at the time. The year 2008 became the turning point, when a memory stick, connected to an army laptop in a military base from the Middle East affected all of the military communication systems (Theiler, O., 2011).

This spyware transferred thousands of classified files which were stored on servers belonging to several states, which were under strict control. Incidentally, the fact that cyber-attacks that come in waves are aimed at strongly developed states is well known, because these states are dependent on communication technologies, thus becoming sure targets due to vulnerabilities.

Through an operation orchestrated by the FBI in cooperation with many countries from Europe and Asia, as well as Australia, it was made possible, through the use of an encrypted application, to arrest a high number of people that were part of a distributed cyber-criminal organisation with members from different corners of the world. These people connected to the application provided by the FBI, trying all kinds of cyber-attacks directed at a number of states, without knowing the fact that their actions were monitored (Europol, 2021).

If it is possible to refer to cybernetic attacks, we can also underline the fact that one of the major cyber-attacks lasted almost 9 months, during which the United States neither knew, nor intervened in order to fight against the cybernetic attack, a fact which proves how dangerous and how difficult to detect they are. This attack took place in the United States when a group of hackers managed to attack one of the most important American federal institutions, by using a software that updated itself (Stergiopoulos, G., Gritzalis, D. & Limnaios, E. 2020).

Another example of a significant cybernetic attack that happened in the United States that has been detected and stopped somewhat late, was against a main fuel supply pipeline. In this context, the national infrastructure

was significantly weakened, creating a critical situation that stemmed directly from the degree to which its operation and control was digitized (Turton, W. & Mehrotra, K., 2021).

We can go on with a significant number of cybernetic attacks which had implications for the US, among which we may recount an incident where a virus stopped operations in hospitals, airports, banks, governmental agencies, and paralysed the naval industry for a period of 7 days, creating immense damage (Cybersecurity and Infrastructure Security Agency, 2021).

In March 2019, a cybernetic attack took place against the energy system of the USA., by exploiting a vulnerability found by hackers, which implied the continuous restart of the firewalls of a network operator, the consequences of this attack being devastating (Stergiopoulos, G., Gritzalis, D. & Limnaios, E. 2020).

One of the most recent and strong cyber-attacks is named Ripple 20, from June 2020, when a group of 19 vulnerabilities affected millions of connected devices, including smart devices, electrical network equipment, health systems, transport systems, mobile communications etc. (Cybersecurity and Infrastructure Security Agency, 2021).

It has been concluded that, globally, in the last few years, the number of cyber-attacks has seen a 30% increase, which is higher than in previous years, and which mainly target industrial control systems like those from the energy industry.

In this context, at a reunion of heads of states from the North Atlantic Treaty Organisation, a document updating and improving the way of response against hybrid and cyber-attacks has been drafted. At the NATO 2030 "Together for a new era" reunion, it has been discussed that such actions should be recognised as attacks in the field of military operations, similar to those in the land, sea and air domains (Lupitu, R., 2020). It also aims to improve the cyber defence, the training of personnel and most importantly, to lead to the drafting of an adequate legal framework, as soon as possible, that is necessary for these problems (NATO, 2020a).

For example, in the case of non-NATO Member States, the current legal frameworks offer adequate means to discourage military development in all fields of operations, only by taking political and military elements into consideration. But, when it comes to cybernetic warfare, the context changes in the sense that there is a multitude of unknown variables. One main question that the Member States of NATO should answer is how to detect cybernetic attacks in a timely manner in order to avoid major implications for the attacked state (NATO Cooperative Cyber Defence Centre of Excellence, 2014).

At the same time, the experience of the cybernetic attack that took place in 2007 in Estonia, and also other situations, led to significant discussions within NATO that concluded that the Article 5 clause for common defence can also be applied in the case of cybernetic war, despite the inherent limitations in knowledge regarding such attacks, their author and their impact.

As previously mentioned, NATO recognises cybernetic space as a field of operations, a subject that was discussed during the Warsaw Summit between 8-9 July 2016, finding international law provisions as applicable while underlining that cybernetic defence is part of the main collective defence task of NATO (Sabbagh, D. & Borger, J., 2021).

In regards to recognizing cybernetic space as one of operational domains, we have to ask the question: "If there are no differences between operational domains, considering the military capacities and capabilities, why are there no offensive measures taken in order to fight against cybernetic attacks?"

Another question would be: "As long as the Warsaw summit underlines the fact that cybernetic space is a domain of operations, why are the provisions of international law from the Geneva Convention from 1949 and its protocols not applicable?"

It has been mentioned numerous times that cybernetic defence and resilience both on NATO and EU levels, as organisations, are the number one priority. This also encompasses NATO actions in cyberspace that are defensive in a proportional way according to the application of international law. This is a reason for NATO establishing a Cybernetic Operations Centre in Mons, Belgium that has the task of coordinating NATO Operations in cyberspace (NATO, 2020b).

At the same time, we can indicate Romania as an important Member State from the cyber perspective, one which is making major progress regarding cybersecurity, which was further highlighted by the selection of Romania to host the European Cybersecurity Competence Centre and Network.

This Centre will play a vital role, considering that cybernetic attacks are more frequent and more aggressive, with a high incidence in the Balkans region as part of a hybrid approach in order to destabilize the South-Eastern and Eastern part of Europe.

We can strongly consider that one of the most important factors in fighting against cybernetic attacks is represented by the partnerships between organisations and consolidating the cooperation between NATO and the EU, in order to support countries in facing the challenges from cybernetic space (The European Union Council, 2020a).

ADOPTING A PROTOCOL V TO THE GENEVA CONVENTION THAT REGULATES THE CYBERNETIC SPACE / WARFARE AS PART OF INTERNATIONAL LAW

At EU level, there is a consensus on the necessity of applying international law provisions, especially the UN charter in its entirety, in the cyber realm. Cybernetic attacks that take place in different places of the world create difficult situations for responders who must prevent and react to these attacks, especially given the lack of norms governing cyberwarfare and adequate responses to it, as well as the lack of a suitable framework for global cooperation in terms of operational security and law enforcement.

The new battlefields are very different from the ones that we knew and recognized in international law, with potentially disastrous attacks being ineligible for reporting as violations of international law.

Moreover, experts from the UN, after more discussions have reached the conclusion that the only method to slow attacks in cybernetic space would be a regulation in international law to enable a response to these incidents.

One of the important subjects discussed by President Joe Biden at the NATO Summit on the 14th of June 2021 is in regards to hybrid actions, ill-intentioned cybernetic activities and also interference against NATO Member States. In this regard, a new cyber security strategy is being drafted as a response against cybernetic attacks with significance and reflection upon the NATO obligation of collective defence (Ministry of External Affairs, 2021).

At the moment, it is necessary to promote a convention or a protocol to support, at international law level, the various initiatives in this field (regulations, treaties, codes of conduct, memoranda, recommendations, standards etc.) and also the organisations (sectoral, technical, civil society) that work at NATO, EU and UN levels.

Also, states can meet and agree upon the amendment of the convention through the introduction of a protocol V that would enable the state and non-state parties to be able to intervene and to defend against cybernetic attacks, through offensive operations in the cybernetic space concomitant with the defeat of attacks, taking cybernetic warfare to another level, that would truly give it the name of cyber war in international law.

Taking into consideration that the risks the state and non-state actors face because of cyber-attacks are very real and becoming more frequent, updating international law becomes mandatory.

At the Brussels Summit from the 14th of June 2021, it was indicated that cybersecurity is both a means and an end for NATO militaries to operate efficiently, when needed, against hybrid actions and cybernetic activities with ill intent, directed at NATO allies and partners. At this summit, a new approach has been taken in regards to the cybernetic attacks, mostly because it has been observed that it is becoming common practice for a State to be "turning a blind eye to cyber criminals operating from its territory, including those who target and disrupt critical infrastructure in NATO countries" (NATO, 2021).

Considering the aforementioned facts, it has not remained unnoticed that the efforts meant to regulate defence in case of cyber-attacks cannot progress unless Member States manage to surpass national limitations and strive towards a common cyber defence policy (Minárik, T., 2017).

More than that, the nature of cyber-attacks and their investigation delays the confident and provable identification of perpetrators and detracts from the efficiency of deterrence frameworks.

From this subject arises the need to modify the Geneva Convention from 1949 and introduce an amendment to Protocol V that supports both state and non-state actors in fighting against cybernetic attacks in the context of hybrid warfare.

DISCUSSIONS

International organisations must cooperate in order to support each other against these cybernetic attacks and to draft rules that increase their protection level. The necessity of this cooperation stems from the obvious insecurity of Member States. Social and economic convergence, as a European ideal, also leads to convergence in cyber development, computer networks, standards used, which also increases the surface area for cyber attackers and their operations. Common approaches to cybersecurity become vital, going all the way to compatible or common legal approaches. As a matter of fact, one of the main problems of the Member States is the lack of correlation in applying the rules and recommendations in developing and exploiting systems and networks, engendering new vulnerabilities. Ultimately, what is needed is the consolidation of cooperation between international organisations with partner countries in order to promote a common direction against cybernetic attacks.

CONCLUSIONS

We mention the fact that a main factor in defending states against cybernetic attacks is a common vision that the Member States and the organisations have in this situation. According to the organisations, cyberspace has become a new operational domain like land, sea or air. However, many analyses show that countries differ in the allocation of resources to fight against cyber threats and in the extent to which they take measures against cyber criminals. These facts may lead to the case where states are unable to take any measures against the cyberattacks that originate from said states. The differences in the rate of development when it comes to cyber defence policies, create increasing difficulties in applying the said policies, which leaves international organisations to create regulations in order to balance the situation and to improve future cybersecurity.

The common vision shared by NATO and the EU can only be beneficial in the sense it is aimed for the implementation of some common rules that support both parties against cybernetic incidents and attacks. Although states and international organisations are drafting orders and recommendations, the big wave of cybernetic attacks, their diversity, their detection and the arduous process of identification of the perpetrators raise important questions for NATO and the EU, not least of which is the subjection of cybernetic and hybrid warfare to international law regulations. The NATO-EU partnership and other organisations'

vision is to improve the legislation in the field of cybersecurity in order to ensure the security of Member States by permanently adapting the legal framework and finding the solutions that support states against the cybernetic attacks, from an operational but also from a governance standpoint. In this sense, it is more frequently invoked that in case of a cybernetic attack with destructive aspects against a state, states should take into consideration invoking Article 5, even without knowing the full extent of the cybernetic attack.

The priorities are to improve response capacity against cybernetic incidents, and, at the same time, to create a vision for future development that enables the defence of states from these attacks, and, if necessary, the offensive actions against perpetrators in real time. As a final conclusion after the analysis of decision elements and factors, of the legal framework of international organisations, it is presumed that a safety element is missing, that would enable a timely intervention and ultimately legally sanction states that do not abide by the regulations.

At this moment, the sanctions imposed by the international organisations are at an economic-financial level, through the introduction of restrictive measures, as well as freezing other avenues for cooperation with NATO-EU countries as a group, with a view towards creating a discouraging and dissuasive effect on states that may sponsor cyber-attacks.

Because of the fact that currently non-EU/NATO states do not agree to follow international recommendations, and the sanctions imposed do not create an adequate incentive to improve their position regarding their cyberspace, it is important to take clear measures to improve the legal framework, in order to allow for the development of suitable cyber capabilities.

In this context, there is nothing left to be done other than to introduce hybrid and cybernetic warfare considerations into international law, by modifying the Geneva Convention. The gravity of the security situation we face is apparent and what is missing is a clear and predictable way to hold perpetrators to account in order to discourage such behaviour.

REFERENCE LIST

Cybersecurity and Infrastructure Security Agency. (2021). *Cybersecurity and physical security convergence guide*. Retrieved 19 June, 2021 from https://www.cisa.gov/sites/default/files/publications/Cybersecurity%20and%20Physical%20Security%20Convergence_508_01.05.2021.pdf

Europol. (2021). *800 criminals arrested in biggest ever law enforcement operation against encrypted communication*. Retrieved 26 June, 2021 from https://www.europol.europa.eu/newsroom/news/800-criminals-arrested-in-biggest-ever-law-enforcement-operation-against-encrypted-communication

Lupitu, R. (2020). NATO 2030 *Report refers to „the most successful alliance from history from the Pacific to the Black Sea" and recommends the consolidation of aggression discouragement for Russia on the eastern flank.* Retrieved 24 June, 2021 from https://www.caleaeuropeana.ro/raportul-nato-2030-face-referire-la-cea-mai-de-succes-alianta-din-istorie-din-pacific-si-pana-la-marea-neagra-si-recomanda-consolidarea-descurajarii-agresiunii-rusiei-pe-flancul-estic/

Minárik, T. (2017). *NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit*. Retrieved 21 June, 2021 from https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit/

Ministry of External Affairs. (2021). *Address from NATO Summit from Bruxelles - 14 June 2021. Retrieved 21 June, 2021* from https://www.mae.ro/node/55924

NATO Cooperative Cyber Defence Centre of Excellence. (2014). *NATO Summit Updates Cyber Defence Policy*. Retrieved 17 June, 2021 from https://ccdcoe.org/incyder-articles/nato-summit-updates-cyber-defence-policy/

NATO. (2020a). *NATO 2030: United for a New Era - "Reflection Group Appointed by the NATO Secretary General"*. Retrieved 20 June, 2021 from https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf

NATO. (2020b). *NATO Cyberdefence Factsheet.* Retrieved 24 June, 2021 from https://www.nato.int/nato_static_fl2014/assets/pdf/2020/8/pdf/2008-factsheet-cyber-defence-en.pdf

NATO. (2021). *Brussels Summit Communiqué- Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels.* Retrieved 25 June, 2021 from https://www.nato.int/cps/en/natohq/news_185000.htm

Publication office of the European Union. (2018). *Security of networks and computer systems - Summary regarding Directive (EU) 2016/1148 regarding security of networks and computer systems.* Retrieved 14 June, 2021 from https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=LEGISSUM:4314915&from=RO

Ranger, S. (2014). *NATO updates cyber defence policy as digital attacks become a standard part of conflict.* Retrieved 30 June, 2021 from https://www.zdnet.com/article/nato-updates-cyber-defence-policy-as-digital-attacks-become-a-standard-part-of-conflict/

Sabbagh, D., & Borger, J. (2021). *Nato summit: leaders declare China presents security risk.* Retrieved June 14, 2021 from https://www.theguardian.com/world/2021/jun/14/nato-summit-china-russia-biden-cyber-attacks

Stergiopoulos, G., Gritzalis, D. & Limnaios, E. (2020). *Cyber-Attacks on the Oil & Gas Sector: A survey on Incident Assessment and Attack Patterns.* Retrieved 16 June, 2021 from https://www.infosec.aueb.gr/Publications/Paper%20J82%20Stergiopoulos%202020.pdf

The European Commission. (2013). *Common communication to the European Parliament, Council, Economic and Social European Committee, and Region Committee - Cybernetic Security Strategy of the European Union: an open, safe and secure cybernetic space.* Retrieved 19 June, 2021 from https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:52013JC0001&from=RO

The European Commission. (2017). *Europe that defends: debate regarding the transition to a union of security and defence.* Retrieved 20 June, 2021 from https://ec.europa.eu/commission/presscorner/detail/ro/IP_17_1516

The European Commission. (2019). Commission Recommendation (EU) 2019/553 on cybersecurity in the energy sector. *Official Journal of the European Union*, 96, 50-54. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.096.01.0050.01.ENG&toc=OJ:L:2019:096:TOC

The European Commission. (2020). *Migration and Home Affairs*. Retrieved 22 June, 2021 from https://ec.europa.eu/home-affairs/what-we-do/policies/cybercrime_en

The European Commission. (2020). *Shaping Europe's digital future - Revised Directive on Security of Network and Information Systems (NIS2).* Retrieved 27 June, 2021 from https://digital-strategy.ec.europa.eu/en/library/revised-directive-security-network-and-information-systems-nis2

The European Court of Auditors. (2019). *Challenges for an effective EU policy in the field of cybernetic security - Information Document.* Retrieved 25 June, 2021 from https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_RO.pdf

The European Parliament and The European Union Council. (2016). Directive (EU) 2016/1148 The European Parliament and Council from 6th of July 2016 regarding measures for a heightened common level of network and computer systems security in the Union. *Official Journal of the European Union, 194/1*, 1-30. https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32016L1148&from=RO

The European Parliament. (2021). *The NIS2 Directive A high common level of cybersecurity in the EU*. Retrieved 20 July, 2021 from https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf

The European Union Council. (2004). Convention of the European Union Council from 23rd of November 2001 regarding cybernetic crimes. *Official Monitor of Romania, 343*. http://legislatie.just.ro/Public/DetaliiDocumentAfis/51289

The European Union Council. (2019a). Decision (PESC) 2019/797 of the Council regarding restrictive measures against cybernetic attacks that represent a threat to the Union or its member states. *Official Journal of the European Union, 129 I*, 13-19. http://www.onpcsb.ro/pdf/Decizia%200797-2019,%20atacuri%20cibernetice.pdf

The European Union Council. (2019b). *A new strategic agenda 2019-2024*. Retrieved 26 June, 2021 from https://www.consilium.europa.eu/ro/press/press-releases/2019/06/20/a-new-strategic-agenda-2019-2024/

The European Union Council. (2020a). *Press release - The new european competency centre for cybernetic security will be based in Bucharest, Romania.* Retrieved 18 June, 2021 from https://www.consilium.europa.eu/ro/press/press-releases/2020/12/10/the-new-european-cybersecurity-competence-centre-to-be-located-in-bucharest-romania/

The European Union Council. (2020b). *A better access to electronic evidence, in regards to fighting crime.* Retrieved 23 June, 2021 from https://www.consilium.europa.eu/ro/policies/e-evidence/

The European Union Council. (2021). *Cybernetic Security: how does the E.U. fight against cybernetic threats.* Retrieved 25 June, 2021 from https://www.consilium.europa.eu/ro/policies/cybersecurity/

Theiler, O. (2011). *New threats: cybernetic dimensions.* Retrieved 16 June, 2021 from https://www.nato.int/docu/review/2011/11-september/cyber-threads/ro/index.htm

Turton, W., & Mehrotra, K. (2021). Cybersecurity - *Hackers Breached Colonial Pipeline Using Compromised Password.* Retrieved 21 June, 2021 from https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password