REGULATORY FRAMEWORK APPLICABLE TO NATO AND THE EU THROUGH CODEPENDENCE

Major Adrian MALDEȘ, Ph.D Candidate[*]

***Abstract**: This paper is the result of an analysis of the international literature aimed at highlighting the interdependence between NATO and the EU in terms of monitoring, optimizing and adopting the regulatory framework that applies at the level of international organizations. Moreover, the optimization and adoption of a common regulatory framework at the level of the organizations in terms of security policy and security regulations that have the force of law is imperative. In this way, the states of the world, which are obliged to comply with the legal provisions on the security of cyberspace, can comply with the obligations and recommendations that play a more informative role to ensure the security of their states, and not only in terms of cyber attacks. Currently, the EU, an international economic organization, is several steps ahead of the international military organization NATO in imposing stricter and tougher measures on European states regarding cyberspace.*

***Keywords**: cyberattacks, legal framework, security policies, international law.*

I.Introduction

The purpose of this paper is to elaborate the essential elements of the codependency of legal frameworks and security policies between NATO and the EU. To this end, a qualitative research method was chosen for this study, involving an exploratory cross-sectional and longitudinal examination of the literature.

The central objectives of this research were to demonstrate the need for a common legal framework at the level of international organisations, to show the differences in the applicability of norms with the force of law at the level of the organisations and the co-dependence between the two major

[*] Navy Staff , email: adi_maldes@yahoo.com.

international organisations NATO and the EU in terms of adopting, monitoring and optimising security policies at the level of each organisation. The collection and analysis of data took place in a context where cyberspace has become the main focal point of our planet, where both state and non-state actors, terrorist, totalitarian or extremist groups have developed cyber actions with a major impact on civil society and not only. For this reason, international organisations have become aware of the risks that vulnerable countries face and have therefore taken the necessary measures to prevent and combat cyber attacks.

Considering the fact that cyber actions are on the rise because an open and free cyber space is sought without violating fundamental rights such as the rule of law, democracy, freedom, etc., international organisations, and not only them, are in a position to introduce new security procedures with a higher risk rate. To ensure the freedom of cyberspace, which would bring great benefits to all states, a solid infrastructure of communication tools and technologies is needed to ensure greater resilience against all types of cyber attacks. Only then can citizens, governments and state institutions benefit from the freedom of cyberspace and its specific advantages. The alarming increase in attacks caused by cybercrime is forcing EU Member States and NATO to change their vision and priorities from this point of view. This means that faster, more efficient and tougher action against malicious attacks from cyberspace is needed. At the same time, countries with underdeveloped infrastructure must receive help and support by finding and applying fast and efficient methods to avoid, as much as possible, the threats and risks they face caused by ransomware attacks in cyberspace[1].

At the European level, the EU (European Union) as a political-economic and social organisation and NATO (North Atlantic Treaty Organisation) as a political-military intergovernmental organisation are

[1] (Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and Committee of the Regions The European Union's cybersecurity strategy: an open, secure cyberspace and secured 2013)

working intensively on the adoption of cooperation measures in the field of security and cyber defence[2].

Under these conditions, all states have understood the importance of ensuring national security in relation to their own sovereignty as well as the security of cyberspace, the latter having become a major international concern due to cybercrime and cyberterrorism. Terrorist and extremist groups, as well as hacker groups, have advanced their skills in the technique of approach, developed cyber capabilities and specialised in large-scale cyber attacks. In this context, international organisations intend to define a common standard procedure to combat cyber attacks and reduce vulnerabilities and threats from cyberspace. The first action taken at the international level is the cooperation between the EU and NATO. These steps lead to a positive contribution for civil society in private-public, economic, political and military environments. This action provides more security and freedom for the development of activities in the virtual environment. The main objective of the cooperation of EU-NATO is to update and harmonise the existing legal and regulatory framework with the security measures implemented by each organisation in order to strengthen the greatest possible international resilience.

In recent years, the cooperation of EU-NATO has brought great benefits, especially during the pandemic COVID -19, which not only made us aware of the discrepancies and habits between security policies, but also the lack of security in cyberspace and broadened our horizons. During this time, cyber-attacks in cyberspace experienced a strong upswing and organisations realised that it was necessary to conclude new international agreements/conventions to stop this rising trend.[3]

II. The regulatory framework of EU security policy in recent years.

The regulatory framework for security policy measures adopted and implemented by the European Union is based on the Treaty on European

[2] European Parliament, 2021, available at https://www.europarl.europa.eu/doceo/document-/TA-9-2021-0412_RO.html, accessed on 21.05.2022.

[3] European Parliament resolution of 7 October 2021 on the state of the EU's cyber defense capabilities (2020/2256 (INI)), 2021.

Union (TEU)[4] and the Treaty on the Functioning of the European Union (TFEU)[5], which, under the provisions of Article 42 et seq. of the EU Treaty on the Common Security and Defence Policy and Article 114 et seq. of the TFEU, confer on the EU the right and competence to take action and to safeguard the security and sovereignty of the Member States.

All these decisions taken by the EU are made in accordance with international law and the principles of the United Nations Charter (UN Charter).[6] At the same time, Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems is the first step in raising EU Member States' awareness of the threat, which is a key element in establishing a common security and safety policy and a normative legal framework that brings together all state actors[7].

It is important to note that in 2004, the EU, through the European Parliament and the Council, established the European Union Cyber Security Agency (ENISA), whose aim is to develop a cyber security culture and ensure a high and effective level of security[8]. As one of the objectives of this body is to achieve a high and common level of security in Europe, its mandate has been extended until the end of 2022. The latter has established the NIS cooperation group and the Informational Security Incident

[4] European Union, Official Journal of the Union, 2012, available at https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6-.0001.02/DOC_1&format=PDF, accessed on 21.05.2022.

[5] European Union, Treaty on the Functioning of the European Union, 2012, available at https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0001.02/DOC_2&format=PDF, accessed on 15.03.2022.

[6] Charter of the United Nations 1945, available at http://www.anr.gov.ro/docs/legislatie-/internationala/Carta_Organizatiei_Natiunilor_Unite_ONU_.pdf, accessed on 15.03.2022.

[7] European Union 2013, available at https://eur--lex-europa-eu.translate.goog/legal-content/EN/ALL/?uri=CELEX:32013L0040&_x_tr_sl=auto&_x_tr_tl=en&_x_tr_hl=ro, accessed on 16.03.2022.

[8] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (European Union Agency for Cyber Security) and on the certification of cyber security in information and communication technology 2019, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2019.151.01.0015.01.ENG-&toc=OJ%3AL%3A2019%3A151%3ATOC, accessed on 16.03.2022.

Response Network (CSIRT) with guidelines for cybersecurity information sharing and cooperation on cybersecurity incidents.

From the legal perspective of the existing legal framework at EU level, we reiterate that under the given conditions, the first effective response to cybersecurity challenges with regard to cyberspace is contained in the Regulations of Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures for a common high level of security of networks and information systems in the Union[9]. According to the NIS directive, improving civil cybersecurity is an important factor and can contribute to the resilience of network and information security at national and international level.

At the national level, Romania, with Law No. 362/2018 on ensuring a high common level of security of networks and information systems, which came into force on 12 January 2019,[10] implements the European Union's Directive on Network Security. This law was adopted late because after more than three years, or 2020, the EU Member States found that the Directive NIS has shortcomings and inconsistencies in its application and thus does not reach the expected level for which it was adopted to ensure a high level of common security. This aspect became even more evident with the Covid 19 pandemic.

At the same time, in December 2021, Romania adopted Government Decision No. 1321 approving the Romanian Cybersecurity Strategy for the period 2022-2027[11], which, considering the repeal of the old GD 271/2003, is supposed to be a cornerstone for cybersecurity in Romania. After a thorough analysis, it turns out that it is only a normative act that takes into

---

[9] Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures for a high common level of security of networks and information systems throughout the Union, 2016, available at https://eur-lex.europa.eu/eli/dir/2016/1148/-oj?locale=en#, accessed on 16.03.2022.

[10] Law no. 362/2018 on ensuring a high common level of security of networks and information systems entered into force on 12 January 2019, available at https://-legislatie.just.ro/Public/DetaliiDocument/209670, accessed on 16.03.2022.

[11] Decision no. 1,321 of December 30, 2021 regarding the approval of the Romanian Cyber Security Strategy, for the period 2022-2027, as well as of the Action Plan for the implementation of the Romanian Cyber Security Strategy, for the period 2022-2027, 2021, available at https://legislatie.just.ro/Public/FormaPrintabila/00000G2NRYHTAYF0PMN2-HT83DEZJYXUZ, accessed on 22.03.2022.

account the needs and requirements of cybersecurity in our country. However, at the national level, there is no law so far that contributes to and supports the measures against cyber attacks required by the EU through European directives, with the exception of a draft law that is still under debate.

Consultations between EU member states have started in mid-2020 to revise the directive NIS. The consultations with EU structures and bodies, in cooperation with representatives of the participating Member States, have identified several shortcomings that could undermine the effectiveness of this directive[12].

The European Union consultations on the adoption of conclusions on the EU Cybersecurity Strategy demonstrate the need and requirements to revise this directive NIS to create a new strong and powerful cybersecurity with the aim of building a resilient and digital Europe. Modeling and adapting international norms and standards in the area of communication and information infrastructures and beyond is essential to the vision of a digital Europe that meets high performance standards while ensuring security in cyberspace[13].

The European Commission and other authorised bodies have put forward several legislative initiatives, including the 16 December 2020 initiative to modernise the existing EU cybersecurity legal framework. The aim of this proposed directive is to implement measures for a high level of cyber security across the Union and to improve the existing EU legal framework, networks and information systems. The agenda discussed by the European Commission's Impact Assessment Board was to analyse the main

[12] Directive of the European Parliament and of the Council on measures for a common high level of cyber security in the Union, repealing Directive (EU) 2016/1148, 2020, available at https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:52020PC0823&-from=EN, accessed on 22.03.2022.

[13] Council of the European Union ,2021, available at https://data.consilium.europa.-eu/doc/document/ST-6722-2021-INIT/en/pdf, accessed on 22.03.2022.

problems in terms of low cyber resilience, inconsistent resilience of Member States and low awareness of the situation by all stakeholders[14].

In fact, the European Commission has put forward a proposal to replace the NIS directive in order to increase safety requirements. The proposed extension aims to force more institutions and sectors to take action to raise the level of cybersecurity in Europe. To ensure greater clarity and coherence with related EU legislation, other initiatives are being considered alongside the revised directive NIS. One of these initiatives relates to the Critical Entity Resilience Directive (ERC), a proposal presented together with the NIS2 Directive to improve the resilience of critical entities to threats.[15]

The new proposals for the NIS2 Directive give ENISA greater responsibility for monitoring and overseeing its implementation, with a mandatory biennial report on the state of cybersecurity in the EU and registration of potential vulnerabilities in a European registry. As a final conclusion after the discussions on the NIS2 proposals by experts in the field, it was noted, given the majority opinion of the Member States, that the application of the European Directive has a much greater impact on a wider range of entities in the field. In this respect, NIS2 can be considered to meet the requirements for a stronger and more visionary basic legal framework for cybersecurity in the EU. ENISA is also constantly issuing cybercrime monitoring reports, which are becoming more prolific, especially in ransomware cases.

With regard to cybercrime, we note that the Directive NIS and the NIS2 proposal call for increased security, in particular for critical infrastructure and security policies of Member States exposed to cyber attacks, and that the EU, through the 2001 Budapest Convention on Cybercrime, takes the necessary legislative measures to criminalise offences committed by third parties, both natural and legal, relating to counterfeiting, fraud, misuse of equipment, damage to the integrity of systems and data in

---

[14] Improving the common level of cyber security, 2021, available at https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/662606/EPRS_BRI(2021)-662606_EN.pdf, accessed on 22.03.2022.

[15] NIS2: a high common level of cyber security in the EU. 2021, available at https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333, accessed on 06.04.2022.

the computer system. To this end, Member States shall adopt, in accordance with their national law, the laws, regulations and administrative provisions necessary for the detection and prosecution of such offences for those who enter the computer system in violation of the provisions of this Convention[16].

On the other hand, the 2001 Budapest Convention on Cybercrime was amended by Additional Protocol No. 1 to take into account racist and xenophobic acts that incite hatred, malice, violence, etc. at various levels of society, depending on the sexual nature, colour or religion in the virtual environment. The proposals of Additional Protocol No. 2 also underline the need for consolidation and cooperation in the field of cybercrime[17].

At the same time, we can note that Additional Protocol No. 2 also supports the NIS 2.0 directive, in the sense that it can be applied by all EU Member States as legislation against cyber-attacks such as ransomware attacks, which have recently become more common[18].

Similar to the NIS 2.0 guideline, the second additional protocol of the Budapest Convention from 2001 also needed more time for implementation due to the COVID 19 pandemic. The pandemic was one of the negative factors affecting the EU, due to the numerous cyber attacks on computer systems as well as attacks related to organised crime. Not to forget the terrorist or extremist attacks on critical infrastructures, which have become more frequent recently. Cyber attacks at the macro level can cause imbalances in many economies of states with low security levels, both through the blocking of computer systems and the loss of data and information.

Following the 2001 Budapest Convention on Cybercrime, a number of regulations have been adopted, the most important of which with direct and significant effect are Directive 2002/58/ EC (Confidentiality and Electronic Communications Directive) and Directive 2016/680 (Data

[16] Council of Europe Convention of 23 November 2001, 2001, available at https://legislatie.just.ro/Public/DetaliiDocumentAfis/51289, accessed on 27.03.2022.

[17] Additional Protocol of 28 January, 2003, available at https://legislatie.just.ro/-Public/DetaliiDocument/105151, accessed on 27.03.2022.

[18] The European Commission, 2021, available at https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:52021PC0718&from=EN, accessed on 27.03.2022.

Protection Enforcement Directive) on the fundamental right of everyone to respect for private and family life and to communications secrecy [19].

On 16/02/2020, the European Parliament and the European Commission held a debate on a package of security measures and policies to improve resilience and response to cyber security and critical infrastructure incidents, the Directive of the European Parliament and of the Council on measures for a high level of cyber security, while repealing Directive 2016/680 (Data Protection Directive on Law Enforcement)[20].

In light of the above, we can conclude that the EU relies on a number of supporting factors to combat cyber attacks by adopting and optimising a cyber-specific legal framework to support Member States and partners to reduce the vulnerabilities and risks they face.

III. The normative framework that has governed the security policy of NATO in recent years.

In order for NATO to support Member States in cyber attacks, it has been necessary to include this operational area of cyberspace alongside the other traditional operational areas. In this context, NATO, as with other operational areas, has adopted provisions on the way of acting that underline that the role of this area is purely defensive. Indeed, NATO highlights the Martens Clause, which states that: "Until a more complete law of war can be worked out, the High Contracting Parties deem it appropriate to state that peoples and belligerents shall remain under the guarantee and rule of the principles of the law of nations as derived from the customs existing between civilised peoples, the laws of humanity and the requirements of the public conscience", which means that cyber-actions, although not found as operational elements in international humanitarian law (IUD), can be classified as an operational area and thus provide invaluable assistance to NATO member states subject to massive cyber-attacks[21].

---

[19] Official Journal of the European Union, 2016, available at https://www.dataprotection.-ro/servlet/ViewDocument?id=1263, accessed on 28.03.2022.

[20] The European Commission, 2020, available at https://eur-lex.europa.eu/legal-content/-RO/TXT/HTML/?uri=CELEX:52020PC0823&from=EN, accessed on 29.03.2022.

[21] The Hague Convention on the Law and Customs of the Land War, 1907, available at https://www.arduph.ro/files/articles/Conven%C8%9Bia%20(Regulamentul%20)%20referit

NATO also plays an important role in working and cooperating with its allies to foster and train competent structures to engage in joint cyber defence activities through the sharing of best practises, real-time information transfer, target development, investment and exercises. It is recognised that NATO strongly supports Member States in protecting critical infrastructure, building resilience and strengthening cyber defence through the implementation of the NATO cyber defence commitments. Over the years, NATO has developed and established contingency centres to make operations more resilient to cyber threats. To this end, the Mons Centre on Cyberspace Operations Centre in Belgium and the NATO Centre for Excellence for Cyber Defence in Tallinn, Estonia, were established[22].

The EU's cyber defence policy and the rapid increase in the number of cyber threats have also forced the organization (NATO) to confirm the applicability of international law to cyberspace. Like the EU, in order to develop its cyber defence capacity and capabilities to protect its own networks and to respond quickly and effectively, NATO has had to establish structures to assist the Organisation in protecting itself from hybrid warfare, cyber attacks and terrorism. One of the structures that serve the organisation in reporting security incidents and disseminating information is the Computer Incident Response Capability (NCIRC). The common approach within the Alliance is to implement national cyber defence capabilities through a NATO planning process. In addition, the Alliance places particular emphasis on training designated personnel in the operation and maintenance of cyber defence communications and information systems. For this purpose, there is the NATO School of Communications and Information Systems in Latina, Italy, and the NATO School in Oberammergau, Germany[23].

The press conference prior to the Secretary-General's Summit of NATO on 11 June 2021 discussed the latest cyber operational areas and the

oare%20la%20legile%20%C5%9Fi%20obiceiurile%20r%C4%83zboiului%20pe%20terestru,%20Haga,%2018%20octombrie%201907.pdf, accessed on 29.03.2022.

[22] NATO cyber defense, 2021, available at https://www.nato.int/nato_static_fl2014/assets/pdf/2021/4/pdf/2104-factsheet-cyber-defence-en.pdf, accessed on 29.03.2022.

[23] NATO cyber defense, 2016.

fact that allies are expected to take a more joint approach to cybersecurity policy NATO. On 3 June 2020, NATO condemned malicious cyber activities that destabilised health services and research facilities during the pandemic COVID -19 in a North Atlantic Council statement on malicious cyber activities. NATO reaffirms its support for allies by using its capabilities, including cybersecurity, to deter and protect all cyberspace as long as allies protect their critical infrastructures and strengthen their resilience and cyber defence, taking into account national responsibilities and competences[24].

Basically, the United Nations intergovernmental organisation addresses cyberspace through joint cyber defence with the aim of protecting critical infrastructure and increasing resilience within the alliance. In recent years, NATO has shown that the method chosen as a form of rapid communication with the organisation's allies to support them is the development of technical agreements, commitments, joint statements, amendments and, not least, the confirmation of mandates. In this way, the Alliance has taken the necessary steps and has been able to improve its cyber defence capabilities. NATO Compared to the EU, the Alliance has training and specialisation schools in this field, which is a great and real help for the organisation, and also supports training programmes in cyber defence through the Science for Peace and Security Programme (SPS)[25].

The Brussels 2021 Summit discussed an important issue in support of a more open policy, the principle of which is based on members' determination to adopt more predictable, secure and comprehensive cyber defence rules to further enhance resilience and deter cyber attacks[26]. With the COVID -19 pandemic, NATO notes the rapid development of a sensitive element spread through cyberspace by fake news or articles on websites that can destabilise the Alliance and influence and weaken Alliance security. When we consider and analyse misinformation as a

[24] North Atlantic Treaty Organization, 2020, available at https://www.nato.int/nato-_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-en.pdf, accessed on 29.03.2022.
[25] North Atlantic Treaty Organization, 2021, available at https://www.nato.int/cps/en/-natohq/topics_85373.htm, accessed on 08.04.2022.
[26] North Atlantic Treaty Organization, 2022, available at https://www.nato.-int/cps/en/natohq/topics_78170.htm, accessed on 10.04.2022.

destabilising factor of the Alliance, from the perspective of the United States of America (USA), we find that there is a Cyberspace Solarium Commission (CSC) at the national level, established by the National Defence Authorisation Act from April 2019.

As of 2019, representatives of the CSC met several times in Congress and discussed initiating some legislative proposals on the defence of critical infrastructure. These legislative proposals of the CSC aim to counter misinformation in cyberspace by proving to be a way of working and, above all, a way of showing a high level of vulnerability and risk for the US and its allies[27] Looking at the approach and implementation of recommendations and proposals in the development of rules at the US level, one finds that action in cyberspace as a vision is different from that in the EU.

The US Commission on Solar Cyberspace (CSC) treats the problem of misinformation as a priority, which has increased greatly recently, also considering the fact that this misinformation in the cyberspace population destabilises the security of the United States. Although misinformation has always existed both in social life and in the online environment, the CSC has noted a much greater increase in misinformation in cyberspace due to the pandemic context of COVID -19[28]. The U.S. National Authorisation Act mandated the CSC to take a unique approach to cyber defence strategy that has significant implications for cyberspace, and to develop a new approach to security policy and related legislation.

The Executive Director of CSC stated in a letter that the 54 legislative proposals that the Commission intends to adopt are for the defence of critical infrastructure in the private and public sectors. By adopting these proposals to implement the deterrence strategy, and by accelerating the implementation process, the nation, private sector companies, governments, U.S. citizens and the Commission hope to be better prepared to protect themselves from adverse actions from cyberspace. The proposed high level goals of the CSC in 2020 were to reform the

[27] US Cyber Space Commission, 2021, available at https://drive.google.com/file/d/-1lpfOQdsHC2ZaawMcB5zeCIaO6y3vNp4p/view, accessed on 12.04.2022.
[28] Idem.

structures and organisation of the US government for cyberspace. Some basic elements of structural reform are distinguished here, such as strengthening the existing legal framework, strengthening critical non-military infrastructures, promoting national resilience, redesigning the cyber ecosystem for greater security and operationalising cybersecurity in the virtual environment[29].

In addition, the events of the last decade have attracted the attention of member states of NATO, particularly the United States, due to a series of incidents since 11 September 2001, followed by other major cyberattacks. In the following years, further major cyberattacks on infrastructure followed in Estonia and in 2008 in Georgia.

The states that took urgent action to address vulnerabilities and risks and draw attention to the impact of state actors were the United Kingdom,[30] which ranked cyberattacks as one of the top four threats to the country's national security, along with the United States [31] which in 2010 also identified the cyber threat as one of the greatest challenges to national security.

Please note that the main cyber security handbook that has contributed to the understanding of cyberspace is the Tallinn Handbook 1.0 and later, more recently, the Tallinn Handbook 2.0. As development management, the Tallinn Handbook 1.0 and 2.0 were also developed at the initiative of the Centre for Excellence for Cooperative Cyber Defence in Tallinn (CCDCOE). In terms of the scope of Tallinn Handbook 1.0, we note that there is a more rigorous and narrow approach to cyber operations, cyber espionage, theft of property, international law and other criminal activities in cyberspace. For perspective, the Tallinn Manual 1.0 treats international and non-international armed conflicts, as well as cyber warfare, as international law because states use force, or more precisely, because cyber

[29] US Cyber Space Commission, 2020, available at https://drive.google.com/file/d/1S5N7-KvjFfxow19kCnPl0nx7Mah8pK0uG/view, accessed on 12.04.2022.
[30] UK National Cyber Security Strategy, 2016, available at https://assets.publishing-.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf, accessed on 15.04.2022.
[31] US National Intelligence Strategy, 2019, available at https://www.newstrategycenter-.ro/wp-content/uploads/2019/07/National_Intelligence_Strategy_2019.pdf, accessed on 15.04.2022.

activities take place in the context of the use of force[32]. This Manual also sets out the responsibilities of States, without prejudice to applicable international obligations [33].

It is very important to understand that the Tallinn 1.0 Manual is not a normative framework or an official position of international organisations, but merely a documentary guide to which several legal experts have contributed in order to find favourable solutions and to help organisations prepare study materials that take into account actions in cyberspace[34].

The Tallinn Manual 2.0 has been substantially amended in several respects, particularly with regard to general rules such as the broader debate on international law applicable to cyber operations. The manual also addresses international law applicable to cyber operations, but not criminal law, domestic commercial law or private international law. We also mention the fact that there are very few treaties that develop such issues of cyber operations, as security policies and much of the existing legal framework are secret documents[35].

Although it is very clearly stated that the two textbooks, Tallinn 1.0 and 2.0, serve as a documentary guide or academic paper and do not represent the views of international organisations or constitute legal norms, it has been shown that the influence of these textbooks has been felt in the mapping and analysis of the discussions and partnerships to which States are party.

The CCDCOE intends to sponsor and support the Tallinn 3.0 Manual, which will revise and expand the 2017 edition of the Tallinn 2.0 Manual in light of State practise and statements on the applicability of international law to cyber operations[36].

---

[32] Tallinn Handbook 1.0 International law applicable to cyber warfare, Cambridge University Press, 2013.
[33] Idem.
[34] Idem.
[35] Tallinn Handbook 2.0 on International Law Applicable to Cyber OperationsCambridge University Press, 2017, p.3.
[36] NATO Cooperative Cyber Defense Center of Excellence, 2021, available at https://ccdcoe.org/research/tallinn-manual/, accessed on 15.04.2022.

Both the CSC and the Tallinn Manual influence the approach of the principles that NATO seeks to apply at the organisational level to assist Member States in raising awareness of critical infrastructure as well as in securing IT networks, especially in the case of misinformation and other false information.

IV. The influence of the EU regulatory framework and security policy on the incidental regulatory framework and security process NATO and vice versa

Regarding the applicability and influence of specific EU and NATO -legal frameworks, we note that international organisations have been trying to find unified cybersecurity solutions over the last decade in the face of increasing numbers of cyber attacks, especially in the recent period dominated by the COVID -19 pandemic. This approach is discussed in meetings between high-level NATO and EU officials as an important and strong response in the field of cyber defence.

One of the ways the two organisations will cooperate is through the exchange of information. The need for cooperation was discussed in the sense that both organisations need support by harmonising and optimising security policies as well as the existing regulatory framework at the level of both parties, with the common task of becoming more resilient to cyber attacks. Another important factor in this meeting is the proposal to cooperate in areas such as the exchange of information through the implementation of the directive NIS[37], through its commitments at the level of the NATO alliance [38].

Another factor is the technical arrangements between CERT-EU and NCIRC, which support and facilitate the necessary exchange of information between the two international organisations and improve this area, while at the same time having the task of preventing, detecting and responding to security incidents [39].

---

[37] European Union, 2016, available at https://eur-lex.europa.eu/legal-content/RO/TXT/?-uri=CELEX%3A32016L1148, accessed on 15.04.2022.

[38] North Atlantic Treaty Organization, 2016, available at https://www.nato.int/cps/en/-natohq/news_138122.htm, accessed on 15.04.2022.

[39] Council of the European Union, 2018, available at https://data.consilium.europa.eu-/doc/document/ST-14413-2018-INIT/ro/pdf, accessed on 20.04.2022.

Indeed, NATO recognises the immediate need to change and accelerate the legal framework and security policy as the Alliance faces increasing hybrid attacks and other asymmetric threats, including high-level misinformation and climate change, that affect Alliance security and protection. It seeks a secure and predictable cyberspace for its allies based on rules [40]. In addition, a White House statement outlined the G7 leaders' approach to cyber threats from cyberspace and criminal ransomware networks.

The response to these ransomware threats is based on the leaders' commitment to work together, strengthen critical infrastructure to slow the influx of malicious ransomware actions, and hold states accountable for allowing cyberattacks[41]. Collaboration with other organizations is critical as cyber threats become more prevalent and know no state borders, including NATO or the EU cooperating and collaborating with the United Nations (UN) and the Organization for Security and Cooperation in Europe (OSCE). As for cyber defense in the private sector, collaboration with industry is the critical element in developing technological innovation as well as expertise in this area[42].

The joint declaration NATO-EU at the NATO summit in Warsaw 2016 is an element that strengthens the cooperation between the two organisations in coordinating security and cyber defence and in combating hybrid actions[43]. It is to be welcomed that both the EU and NATO, through cooperation and joint efforts, seek to make a positive contribution to Member States to help them strengthen the protection and resilience of

---

[40] North Atlantic Treaty Organization 2021, available at https://www.nato.int/cps-/en/natohq/news_185000.htm, accessed on 20.04.2022..

[41] White House USA. 2021, available at https://www.whitehouse.gov/briefing-room/-statements-releases/2021/06/13/carbis-bay-g7-summit-communique/, accessed on 21.04.2022.

[42] NATO cyber defense 2016, available at https://www.nato.int/nato_static_fl2014/-assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-en.pdf, accessed on 25.04.2022.

[43] European Council, 2016, available at https://www.consilium.europa.eu/en/-meetings/international-summit/2016/07/08-09/, accessed on 27.04.2022.

critical infrastructures and optimise the legal framework for combating cyber attacks.

Regarding the influence of the legal framework and security policies at the level of the two international organisations, it can be noted that the EU chooses a narrower style in terms of the applicability of the incidental legal framework and security policies, which only apply to EU states with the rule of law and contain binding elements. At the same time, the incidental legal framework applicable to the security policy of NATO refers to the strengthening of cyber defence capabilities as well as to the reaffirmation of the commitment to act in accordance with international humanitarian law (IHL) and the Charter of UN.

In this context, we can note that the security policies and normative framework applicable to NATO cover a broad spectrum that is highly applicable to critical infrastructure, and that they have equal application in member states through the elaboration of commitments/partnerships or technical agreements between international organisations as well as between NATO member states, without having the force of law. The US Congress, through CSC, taking into account the provisions of Tallinn Manuals 1.0 and 2.0, has the task of opening up a new vision for the new Tallinn Guide/Manual 3.0. This is beneficial for NATO as legal experts discuss all security incidents to date and the likelihood of new incidents in the future, leading to a more coherent and clear analysis of potential vulnerabilities and threats from cyberspace in Member States.

V. Conclusions

The conclusions show that both NATO and the EU understand that cyberspace is the new field of operations, the new war zone, and that cooperation between the two international organisations is essential to create a free, just, digital Europe in the virtual environment and an ecologically resilient and cyber-resistant NATO alliance.

Following the summits, the EU adopted conventions and directives with legal effect in a limited framework, specifically for the Member States of the European Union. In this context, legislation and security policies become binding, with deadlines to be respected and taken into account by the states.

Only in a rigorous and robust manner can the provisions of the EU legal framework and security policies be applied while Member States can enjoy the freedom to operate in an open, safe and secure cyberspace. In addition to the existing legal framework, which is updated and optimised as needed, the EU also supports Member States through structures designed and intended for the development of critical infrastructures in less developed countries in order to strengthen their resilience and robustness.

On the other hand, given the complexity of the Allies' approach, NATO takes a broader approach with a more comprehensive vision. So far, NATO has reaffirmed its commitments and agreements with several amendments, one of which stipulates that each state is personally involved in the development of critical infrastructure. This is the only way that NATO member states will be able to defend against and withstand malicious attacks from cyberspace.

NATO also wanted to raise the cyber domain to a higher level through the Martens Clause, so that it would be one of the five traditional domains to which international humanitarian law applies through the Geneva Convention and its Additional Protocols. Instead, the EU is taking a different approach and, after complying with a number of conventions, is launching the NIS and NIS2 directives and the cybercrime directive, which aim to minimise risks and vulnerabilities in cyberspace.

If Member States do not comply and enforce the necessary regulations, they will suffer the consequences of cyber attacks. This research aims to show that in the near future, all international organisations will have common, stricter modalities in what is included in the incident legal regulatory framework and security policy, the influence of guidelines, conventions and protocols along with the security policy of the EU, which is a higher yield, in this successfully in ensuring the obligations of the right states and the agreements within the NATO-EU alliance.

The desire to further refine these international organisations in a common trend, focusing on the rapid and efficient adoption of optimal legislation is a very important asset in a society where globalisation is the main element.

BIBLIOGRAPHY

Additional Protocol of 28 January. 28 01 2003, available at https://legislatie.-just.ro/Public/DetaliiDocument/105151.

MEIROȘU C, ȘUBERNIȚCHI V., *Centrul Român de Politici Europene.* 11 2020, available at https://www.crpe.ro/wp-content/uploads-/2020/12/CRPE_nato_ro-1-1.pdf.

Charter of the United Nations, 26 o6 1945, available at http://www.anr.gov.ro/docs/legislatie/internationala/Carta_-Organizatiei_Natiunilor_Unite_ONU_.pdf.

Comunicare comună către Parlamentul European, Consiliu, Comitetul economic și social European și Comitetul Regiunilor Strategia de securitate cibernetică a Uniunii Europene: un spațiu cibernetic deschis, sigur și securizat, 01 01 2013, available at https://eur-lex.europa.eu/legal-content/RO/TXT/-?uri=celex%3A52013JC0001.

Council of Europe Convention of 23 November 2001. 23 10 2001, available at https://legislatie.just.ro/Public/DetaliiDocumentAfis/-51289.

Council of the European Union. 09 03 2021, available at https://data.-consilium.europa.eu/doc/document/ST-6722-2021-INIT/en/pdf.

Council of the European Union. 19 11 2018, available at https://data.-consilium.europa.eu/doc/document/ST-14413-2018-INIT/-ro/pdf.

Decision no. 1,321 of December 30, 2021 regarding the approval of the Romanian Cyber Security Strategy, for the period 2022-2027, as well as of the Action Plan for the implementation of the Romanian Cyber Security Strategy, for the period 2022-2027. 30 12 2021, available at https://legislatie.just.ro/Public/-FormaPrintabila/00000G2NRYHTAYF0PMN2HT83DEZJYXUZ.

Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures for a high common level of security of

networks and information systems throughout the Union. 06 07 2016, available at https://eur-lex.europa.eu/eli/-dir/2016/1148/oj?locale=en#).

Directive of the European Parliament and of the Council on measures for a common high level of cyber security in the Union, repealing Directive (EU) 2016/1148. 16 12 2020, available at https://eur-lex.europa.eu/legal-content/RO/TXT/HTML-/?uri=CELEX:52020PC0823&from=EN.

European Council. 08 07 2016, available at https://www.consilium.europa.-eu/en/meetings/international-summit/2016/07/08-09/ .

European Parliament. 07 10 2021, available at https://www.europarl.-europa.eu/doceo/document/TA-9-2021-0412_RO.html.

European Union. 12 08 2013, available at https://eur--lex-europa-eu.-translate.goog/legal-content/EN/ALL/?uri=CELEX:-32013L0040&_x_tr_sl=auto&_x_tr_tl=en&_x_tr_hl=ro.

European Union. 06 07 2016, available at https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32016L1148.

European Union, Official Journal of the Union. *Treaty on European Union.* 26 10 2012, available at https://eur-lex.europa.eu/resource-.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6-.0001.02/DOC_1&format=PDF.

Treaty on the Functioning of the European Union. 26 10 2012, available at https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0001.02/DOC_2&format=-PDF.

Improving the common level of cyber security. 02 2021, available at https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/-662606/EPRS_BRI(2021)662606_EN.pdf.

Joint Communication To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. 01 2013, available at https://eur-lex.europa.eu/legal-content/-EN/TXT/?uri=celex%3A52013JC0001.

Jurnalul Oficial al Uniunii Europene. 13 06 2018, available at https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:-52018IP0258&from=IT.

Law no. 362/2018 on ensuring a high common level of security of networks and information systems entered into force on 12 January 2019, 28 12 2018, available at https://legislatie.just.ro/Public-/DetaliiDocument/209670.

NATO Cooperative Cyber Defense Center of Excellence, 2021, available at https://ccdcoe.org/research/tallinn-manual/.

NATO cyber defense, 10 04 2021, available at https://www.nato.int/nato_-static_fl2014/assets/pdf/2021/4/pdf/2104-factsheet-cyber-defence-en.pdf.

NATO cyber defense, 12 04 2016, available at https://www.nato.int/nato_-static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-en.pdf.

NATO cyber defense, 07 2016, available at https://www.nato.int/nato_static-_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-en.pdf.

NIS2: a high common level of cyber security in the EU, 01 12 2021, available at https://www.europarl.europa.eu/thinktank/en/-document/EPRS_BRI(2021)689333.

North Atlantic Treaty Organization, 11 06 2021, available at https://-www.nato.int/cps/en/natohq/opinions_184908.htm?selected-Locale=en.

North Atlantic Treaty Organization, 03 06 2020, available at https://www.-nato.int/cps/en/natohq/official_texts_176136.htm?selected-Locale=en.

North Atlantic Treaty Organization, 10 06 2021, available at https://www.-nato.int/cps/en/natohq/topics_85373.htm.

North Atlantic Treaty Organization, 23 03 2022, available at https://www.-nato.int/cps/en/natohq/topics_78170.htm.

North Atlantic Treaty Organization, 25 11 2016, available at https://www.-nato.int/cps/en/natohq/news_138122.htm.

North Atlantic Treaty Organization, 14 06 2021, available at https://www.-nato.int/cps/en/natohq/news_185000.htm.

Official Journal of the European Union, 27 04 2016, available at https://-www.dataprotection.ro/servlet/ViewDocument?id=1263.

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (European Union Agency for Cyber Security) and on the certification of cyber security in information and communication technology, 17 04 2019, available at https://eur-lex.europa.eu/legal-content/EN/TXT-/?uri=uriserv%3AOJ.L_.2019.151.01.0015.01.ENG-&toc=OJ%3AL%3A2019%3A151%3ATOC.

Rezoluția Parlamentului European din 7 octombrie 2021 referitoare la situația capabilităților de apărare cibernetică ale UE (2020/2256(INI)). 7 10 2021, available at https://www.-europarl.europa.eu/doceo/document/TA-9-2021-0412_-RO.html

„Tallinn Handbook 1.0 International law applicable to cyber warfare." 17-18, Cambridge University Press, 2013.

„Tallinn Handbook 2.0 on International Law Applicable to Cyber Operations, Cambridge University Press, 2017.

The European Commission. 25 11 2021, available at https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=-CELEX:52021PC0718&from=EN.

The European Commission, 16 12 2020, available at https://eur-lex.-europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX-:52020PC0823&from=EN.

The Hague Convention on the Law and Customs of the Land War, 18 10 1907, available at https://www.arduph.ro/files/articles/-Conven%C8%9Bia%20(Regulamentul%20)%20referitoare%20la%20legile%20%C5%9Fi%20obiceiurile%20r%C4%83zboiului%20pe%20terestru,%20Haga,%2018%20octombrie%201907.pdf.

UK National Cyber Security Strategy, 2016, available at https://-assets.publishing.service.gov.uk/government/uploads/system-/uploads/attachment_data/file/567242/natinal_cyber_security_strategy_2016.pdf.

US Cyber Space Commission, 12 2021, available at https://drive.google.-com/file/d/1lpfOQdsHC2ZaawMcB5zeCIaO6y3vNp4p/view.
US Cyber Space Commission, 07 2020, available at https://drive.google-.com/file/d/1S5N7KvjFfxow19kCnPl0nx7Mah8pK0uG/view.
US National Intelligence Strategy, 2019, available at https://www.-newstrategycenter.ro/wp-content/uploads/2019/07/National-_Intelligence_Strategy_2019.pdf.
White House USA, 13 06 2021, available at https://www.whitehouse-.gov/briefing-room/statements-releases/2021/06/13/carbis-bay-g7-summit-communique.