Damjan Štrucl
DOI:10.33179/BSV.99.SVI.11.CMC.23.2.2

# PARTNERSTVO MED EU IN NATOM PRI ZAGOTAVLJANJU INFORMACIJSKE OZIROMA KIBERNETSKE VARNOSTI: TEORIJA IN PRAKSA

# THE EU-NATO PARTNERSHIP AND ENSURING INFORMATION SECURITY AND CYBERSECURITY: THEORY AND PRACTICE

**Povzetek** Evropska unija in Nato sta pomembni politični, gospodarski in varnostni organizaciji v globalnem okolju. Razvoj informacijsko-komunikacijske tehnologije in novi izzivi sodobnega varnostnega okolja so povzročili podpis Skupne izjave o poglobljenem strateškem partnerstvu med organizacijama. Obe organizaciji se zavedata svoje vloge in tudi pomembnosti sodelovanja pri zagotavljanju varnosti, še posebej, ker so varnostni izzivi, tveganja in grožnje prepleteni z virtualnim in fizičnim prostorom. S tem prispevkom želimo analizirati strateško partnerstvo med EU in Natom pri zagotavljanju varnosti in obrambe v sodobnem varnostnem okolju, ki temelji na skupni izjavi iz leta 2016.

**Ključne besede** ***Sodelovanje med EU in Natom, varnostno okolje, informacijsko okolje, kibernetska varnost, kibernetski prostor.***

**Abstract** The EU and NATO are important political and security organizations in a global environment. The development of ICT and the new challenges of the contemporary security environment have led to the signing of a joint EU-NATO declaration. Both organizations are aware of their roles, and of the importance of working together to ensure security, especially as security challenges, risks, and threats are intertwined with both virtual and physical space. With this paper, we wish to analyze the EU-NATO strategic partnership in ensuring security and defence in the contemporary security environment, based on a joint statement from 2016.

**Key words** ***NATO-EU cooperation, security environment, information environment, cybersecurity, cyberspace.***

## Introduction

Today, we can no longer imagine the functioning of a global community, states, critical infrastructure or the economy without information and communication technology (ICT). The development of the internet, ICT, the information environment and cyberspace has made society more connected and interdependent, but also more vulnerable. These facts have led to changes in the security environment, resulting in the need for a comprehensive approach to addressing security issues. National borders have become blurred, as the information environment and cyberspace know no physical borders. It is also extremely difficult to identify adversaries or violators of national and/or international law with an adequate level of certainty.

The fact is that today's security environment is complex, as states and the international community concurrently confront the security issues of intertwined virtual and physical space and the consequences of threats that are always transferred from the virtual to the physical space, where the damage occurs. Unlike the physical dimensions of space, virtual space is not regulated; there is no sovereign exercise of power and no established international legal norms (Mačák, in Pissanidis et al., 2016, pp 131-132), the attribution of illegal acts (actors) is almost impossible (Ibid., p 30; Ibid., p 124), it is extremely difficult to manage and control, and the consequences can be global. Thus, in a contemporary security environment, modern society confronts new forms of threats, risks, and challenges which require national and international organizations to take a comprehensive and coordinated approach to ensure all forms of security.

Individual approaches to national security in the information environment and cyberspace alone are insufficient and ineffective (Ibid., p 128). Today we experience cyber incidents and information activities in various forms (especially social engineering and fake news) daily, just at the national level alone, which cannot be limited or prevented. Mogherini (in Rehrl, 2018, p 6) advocates that cooperation between countries is particularly important to achieve resilience to such threats. At the same time, it should be borne in mind that information security, and thus cyber security, is primarily the responsibility of the state. In this manner the state primarily protects its own security, and indirectly international security, as cyber incidents can otherwise be spread uncontrollably beyond national borders (Pernik, 2014, p 7; Mogherini, in Rehrl, 2018, p 6).

Cooperation between countries and organizations is also crucial in ensuring information or cyber security. The European Union (EU) and NATO both advocate a holistic and common approach from the international community in addressing contemporary security issues and the need to share information, design common standards, build trust, and so on, at the political-strategic, operational, and technical (tactical) levels (Relations with the European Union, NATO, 2020, e-source). For this reason, the two organizations signed a Joint Declaration on a strategic partnership, with which they want to achieve a unified approach to their response to contemporary security threats.

In this paper, we will test the hypothesis that effective Euro-Atlantic security requires a unified approach to addressing the security challenges and threats of a contemporary security environment based on transparency and trust. We will achieve this through an analytical approach and the use of deduction, as well as descriptive methods that represent an EU-NATO partnership in cooperation in providing information/cyber security (and defence), or jointly responding to contemporary threats.

## 1 THE EVOLUTION OF THE EU-NATO STRATEGIC PARTNERSHIP: RESPONDING TO CONTEMPORARY SECURITY THREATS

The EU and NATO are important political and military international organizations, directly and indirectly integrated into all three systems of contemporary security: cooperative security, collective security and defence. Both organizations directly ensure their members have collective security and defence[1], and at the same time enable the implementation of the concept of global security (Cohen, 2008, pp 6-7). The EU and NATO share common values[2] and strategic interests, and confront and tackle the same threats and challenges (Lisbon Summit Declaration, NATO, 2010, e-source). Therefore, the organizations are key partners for one another across issues of common interest, crisis management, capability development, and policy consultations on the contemporary security environment (Grissom, 2018, p 1; UL EU C 202/1).

### 1.1 Historical milestones of EU-NATO cooperation in ensuring information/ cyber security

The EU and NATO have long ceased to be the organizations they once were. The changed political environment, globalization, and the development of ICT have shaped global values, sources of threat, and challenges, while at the same time some security issues have become global (Svete, 2005, p 80). Global security issues can include hybrid threats, the information environment, cyberspace, and critical infrastructure, among others. It is precisely these global security issues that are the common denominator of their interconnection and cooperation, as the Member States of the organizations confront the same vectors of threat (both state and non-state actors) that threaten political, economic, and military, as well as civilian, security (Lété in Pernik, 2017, p 1)

The two organizations constantly face serious challenges and threats from the contemporary security environment. The information revolution has led to the need for information assurance, information and cyber security, and the identification of

[1] *Based on the 42 (7) Article of the EU Treaty (Lisbon Treaty), EU Member States shall provide assistance and support to an attacked state by all means available (UL EU, C 202/38, 7. 6. 2016). This provision is complemented by Article 222 of the Treaty on the Functioning of the EU, which stipulates a solidarity clause on joint action by the EU Member States in the event of a terrorist attack, natural disaster, or manmade disaster (UL EU, C 202/1).*

[2] *According to the North Atlantic Treaty and the EU Treaty, these common values are the protection of the rule of law, fundamental human rights and freedoms, democracy, and a common heritage (UL EU, C 202/1).*

new critical sectors of society. Herrmann named these sectors critical infrastructure systems[3] and categorized them as follows: 1. Telecommunications systems; 2. Banking/financial systems; 3. The water supply system; 4. The gas and oil supply and storage system; 5. Power plants and the electricity supply; 6. The transport system; 7. Emergency services; and 8. Government services (2001, pp 1-10). This type of identification of critical infrastructure systems has led to other forms of security, such as operational security, industrial security, technical security, information security, communication and computer security, cybersecurity, network and information security, and so on (ACO Security Directive, AD 70-1, 2012; ENISA overview of cybersecurity and related terminology, ENISA, 2017, p 6).

Although both organizations had identified cyber threats and challenges as early as 2002 (NATO) and 2003 (EU), informal political-strategic cooperation on cyberspace was only established in 2010 and 2011 at the EU-NATO level in response to computer incidents[4]. Their formal cooperation only began in 2016, with the signing of a Technical Agreement on cyber defence between NATO's Computer Incident Response Capability (NCIRC) and the EU Computer Incident Response Team (CERT-EU) (EU and NATO increase information sharing on cyber incidents, EEAS, 2016, e-source).

In the same year, the signing of the Technical Agreement was followed by the signing of the Joint Declaration in Warsaw on the renewed EU-NATO Strategic Partnership. The two organizations agreed that only together could they successfully counter today's global threats, including combating hybrid threats, cyber defence, and enhancing the stability of their partners and neighbours as their security is interconnected (Joint Declaration, EU, 2016, e-source). In 2016 and 2017, Annexes to this Joint Declaration were also adopted, setting out concrete measures to counter hybrid threats, operational cooperation (including maritime issues), cyber defence capabilities, the defence industry and research, exercises, capacity-building, and strengthening political dialogue (Council Conclusions on the Implementation of the Joint Declaration, EU, 2016, 2017, e-source).

The renewed Joint Declaration on the EU-NATO Strategic Partnership was adopted in 2018, reaffirming the implementation of the agreed objectives and goals from 2016. Since both organizations were facing multiple and evolving security challenges, a new commitment to deepening cooperation within the existing common proposals was agreed, including in responding to hybrid and cyber threats. In addition, a new Joint Declaration highlighted the promotion of a fair sharing of the burden, the

---

[3] *Today, these systems are called critical infrastructure, and they must be separated from information infrastructure. The concept of critical infrastructure is much broader and includes critical sectors, while the concept of information infrastructure is linked to the operation of critical infrastructure services (Svete, 2007, p 160). The critical infrastructure of the Republic of Slovenia involves: transport, energy supply and drinking water, finance, healthcare, food, environmental protection and communication information networks and systems (Official Gazette of the Republic of Slovenia, No 75/17).*

[4] *The computer incident response team can be CERT or CSIRT and is generally dedicated to responding to cyber incidents. (Defining Computer Security Incident Response Teams, US-CERT, e-source)*

benefits and responsibilities of the Allies, and the EU's commitment to prioritizing security and defence in future discussions on the next long-term EU budget (Joint Declaration on EU-NATO Cooperation by the President of the European Council, NATO, 2018, e-source).

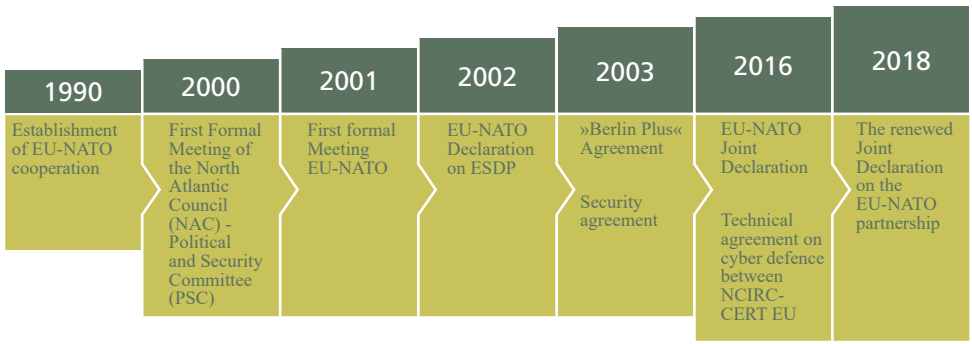



Figure 1: Formal EU-NATO cooperation (Source: extracted from NATO and EU documents)

## 2 AREAS OF EU-NATO COOPERATION

A series of events have shown the true dimensions of the challenges to the information environment and cyberspace, including the cyber-attack on Estonia in 2007, the illegal annexation of Crimea in 2014, the hybrid war in Ukraine, and the 2016 US presidential election (Latici, 2020, p 4). In addition to the common values, all these mentioned events have at least one more shared feature: they have implications for the 21 countries that are members of both the EU and NATO. Of course, we should not ignore the fact that there are other, even more specific political-strategic reasons: 1. The EU needs NATO to ensure military security (NATO's policy of deterrence); 2. NATO needs an EU contribution to the development of European defence capabilities (Europe can become a more relevant transatlantic partner, which makes NATO stronger); 3. The two organizations need each other to confront hybrid threats (the EU has broader competencies); 4. Both organizations are needed to stabilize peace and security in the Euro-Atlantic area (the EU has “soft power” tools to support NATO's »hard power«); and 5. Both organizations need the cooperation of Non-Member States (states who are not members of both organizations) to ensure security in the region. (Latici, 2020, p 4; Raik in Järvenpää, 2017, pp 1-2)

In 2016, the organizations took a key step towards formalizing enhanced cooperation by signing a Joint Declaration, at the same time reaffirming their awareness of common challenges (Latici, 2020, p 4; Raik in Järvenpää, 2017, p 1). The enhanced strategic partnership sets out seven strategic objectives in the areas of operational cooperation, hybrid threats, cybersecurity, defence capabilities, defence capacity building, the defence industry and development, and exercises (Joint Declaration,

EU, 2016, e-source). The Joint Declaration was followed by two Annexes with a total of 74 concrete measures to achieve the strategic goals, emphasizing that NATO remains the transatlantic framework for a strong collective defence and an essential security forum among the Allies. In any case, the strategic partnership is also important for the EU, as it enables more efficient development of the EU's defence capabilities and thus also strengthens NATO (Statement on the Implementation of the Joint Declaration, NATO, 2016, e-source).

**Political-strategic cooperation**

Political and diplomatic cooperation is the basis for the development of international relations and their formalization. This is also confirmed by the joint statement adopted in 2016, in which the organizations stressed the need to protect their common values and interests, which can be achieved through regular formal and informal meetings between the Political and Security Committee (PSC) and the North Atlantic Treaty Organization (NAC) and by enhanced cross-sectoral meetings of relevant committees and councils. (Statement on the Implementation of the Joint Declaration, NATO, 2016, e-source). Additionally, the need to fully involve non-EU Allies in political and diplomatic cooperation was also accepted, which is an important element in developing an international »comprehensive approach« to crisis management and operations. To this end, a decision has been taken to hold regular meetings on issues of common interest at the level of Foreign Ministers, Ambassadors, Military Representatives, and Defence Advisers. For more effective cooperation and coordination, cooperation mechanisms have also been established at all levels between NATO's International Military Staff and the EU institutions (European External Action Service (EEAS), European Defence Agency (EDA)[5], the European Commission and the European Parliament) (NATO-EU Relations Fact Sheet, NATO, 2016, e-source; NATO-EU Relations Fact Sheet, NATO, 2019, e-source).

**Operational cooperation**

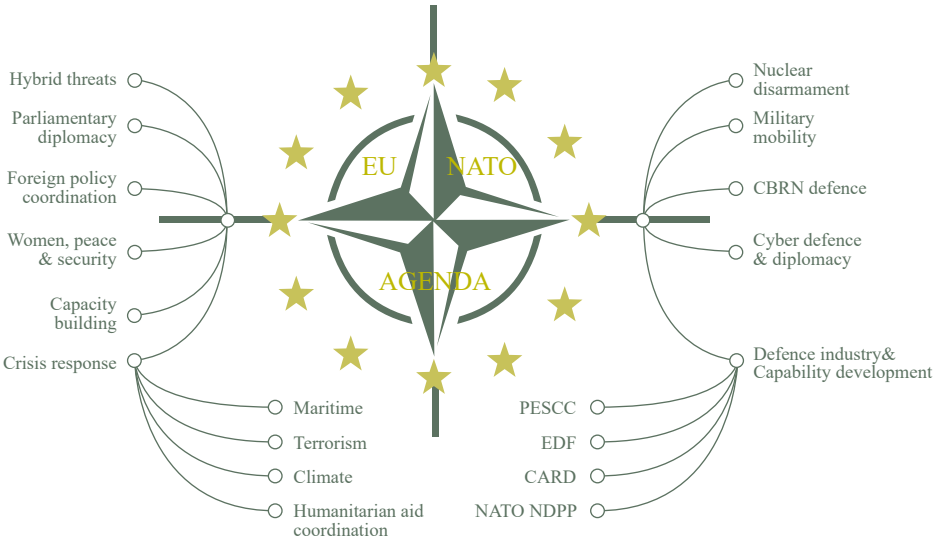
The two organizations established operational cooperation as early as 2005 and 2006, when they set up liaison teams at the EU military staff and NATO's Supreme Headquarters Allied Powers Europe (SHAPE). The adoption of the Joint Declaration strengthened operational cooperation, as it agreed to establish mechanisms for permanent cooperation at all operational levels across all domains of warfare (land, air, sea, space, and cyberspace). In this way the cooperation will include all seven common objectives of the Joint Declaration[6], both in the planning of joint actions

[5] *The EDA is responsible for the area of research and technology, and for cyber defence development. In addition, it provides support to the Member States in developing a skilled military cyber defence workforce, ensures the availability of proactive and reactive cyber defence technology, develops various courses, and raises awareness of CDSP operations (NATO Cyber Defence, EDA, 2020). For education, training, exercises, and evaluation (ETEE), a cybersecurity platform has been established, run by the European Security and Defence College (ESDC) (Cyber platform for Education, Training, Evaluation and Exercise (ETEE), EDA, 2018).*

[6] *Operational cooperation, hybrid, cybersecurity, defence capabilities, defence capacity building, defence industry, development and exercises (Joint Declaration, EU, 2016, e-source).*

and operations and in their implementation (Statement on the Implementation of the Joint Declaration, NATO, 2016, e-source).

Figure 2: EU-NATO Agenda (Source: Latici, 2020, p 5)




## Countering hybrid threats

Awareness of the dangers of hybrid threats and the importance of joint cooperation in countering them is one of the most important areas of both joint statements. Cooperation is based on the implementation and operationalization[7] of parallel procedures and manuals in the areas of web security, strategic communication (Stratcom[8]), crisis response, situational awareness, and building resilience. The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) and the NATO Strategic Communications Centre of Excellence (StratCom CoE) have been identified as key actors in assisting Member States and the two organizations in responding to hybrid threats. In addition, the Hybrid CoE and the StratCom CoE, in cooperation with both military personnel, support Member States and both organizations in strengthening resilience to hybrid threats. In this regard, the following measures have been taken:

– Situational awareness and strategic communications encompass all five domains of space, including the information environment (social media), and cover the systematic exchange of information, analysis, and enhanced cooperation between

[7] *Operationalization: to make something useful and effective in the process; to make operational*

[8] *Stratcom – strategic communications are a coordination function at the strategic level, intended for the analysis and coordination of the communication and information capabilities of the adversary and the complex operational environment (LePafe, 2014, p 6).*

the StratCom CoE and the EEAS Stratcom, and between the newly formed EU Fusion Cell and the relevant NATO entity;
– Crisis response is based on the synchronization of the EU crisis response processes, including the EU's Integrated Political Crisis Response (IPCR) arrangements and the NATO Crisis Response System;
– Strengthening resilience includes regular awareness and cross-reporting on resilience and defining criteria and guidelines for greater coherence between the EU Capability Development Plan (CDP) and the NATO Defence Planning Process (NDPP) (Statement on the Implementation of the Joint Declaration, NATO, 2016, e-source).

**Cybersecurity and defence**

Cyberspace, or the information environment, is a medium for the creation and implementation of hybrid, information, and cyber operations. The organizations agreed to strengthen cooperation in cybersecurity in the area of training and education, including participation in cyber exercises[9]. As an additional measure of cooperation, the exchange of cyber defence concepts was also defined, to promote the interoperability of cyber defence requirements and standards between the two organizations. Another important joint action is cooperation in research and technological innovation of cyber defence, which also enables the interoperability of standards, and is rational in terms of resource consumption (Statement on the Implementation of the Joint Declaration, NATO, 2016, e-source).

**Defence capabilities**

In a joint statement, the organizations adopted the principles of non-duplication and the complementary nature of capabilities. This can only be achieved by ensuring consistency of results between the NDPP and the CDP. The organizations also took additional measures related to complementing multinational projects/programmes developed within NATO Smart Defence and EU Pooling & Sharing, in areas of common interest (satellite communications, cyber defence, remote-controlled aviation systems, etc.) and in the field of standardization (Statement on the Implementation of the Joint Declaration, NATO, 2016, e-source). Through these measures, the two organizations have enabled the unified development of the defence capabilities of the Member States based on the same standards, which is particularly important in responding to modern security threats.

**Education, training, and exercises**

Education, training, and exercises are among the most important areas for strengthening a unified approach to confronting challenges in the modern security environment, concurrently leading to the rationalization of resources. The EU and NATO have agreed to conduct joint education and training in hybrid threats and cybersecurity, as well as to exchange exercise reports and lessons learned. Among

[9] *For example, the »Cyber Coalition« and »Cyber Europe« exercises.*

the measures taken is the cooperation of the two organizations in exercises which include elements of hybrid and cyber threats, based on the principle of parallel and coordinated exercises (PACE), such as crisis response exercises (CMX) and »Cyber Coalition« (Statement on the Implementation of the Joint Declaration, NATO, 2016, e-source).

**Defence capacity building, the defence industry, and research**

This area of cooperation is based on both political-strategic cooperation measures and measures of a non-political nature. Political-strategic measures are aimed at enhanced formal and informal PSC-NCS cooperation and the strengthening of political dialogue, which are the basis for measures of a non-political nature at the operational level. The following were identified as concrete measures of a non-political nature: 1. The identification of possible cooperation projects; 2. Exchange of knowledge between Centres of Excellence and professional staff; 3. Enhanced EU-NATO cooperation in research and technology; and 4. The use of existing forums to develop a dialogue between EU-NATO personnel in the defence industry (Statement on the Implementation of the Joint Declaration, NATO, 2016, e-source).

Political-strategic measures are thus aimed at enhanced formal and informal cooperation between the PSC-NCS and the strengthening of political dialogue, which are the basis for the implementation of non-political nature.

## 2.1 From theory to practice

Monitoring the implementation of the adopted documents is only possible if the implementation of the enclosed provisions/agreements themselves is monitored, which both organizations are aware of. However, just because something is written, does not mean it is done. The actual implementation of the measures demonstrates how seriously the two organizations have taken the agreement, and how credible a partner they are to each other and the Member States. This is also demonstrated by the fact that despite an agreement to produce reports on an annual basis, the organizations produced the first three reports at half-yearly intervals (June 2017, November 2017, May 2018) and only the last two at annual intervals (June 2019, June 2020) as agreed. In writing this, the author would like to emphasize that the discussion is limited to those essential measures that are related to the information environment and cyberspace.

**Political-strategic cooperation**

None of the five reports contain concrete actions taken in this area, but set out general findings of progress, such as strengthening the EU-NATO strategic partnership, common values and interests, burden-sharing, common challenges and threats, strengthening the ESDP, and complementarity between the two organizations (1 - 5 Progress Report on the Implementation of the Common Set of Proposals endorsed by NATO and EU Councils on 6 December 2016/2017, NATO/EU). This is considered normal, as the political-strategic level provides guidelines to be implemented

at the operational level. The policy-strategic guidelines thus assist planning for mutual cooperation at the operational level. This is confirmed by the second and third reports, which state that the PSC-NAC's regular bilateral dialogue on issues of common interest has become the norm, resulting in clear political commitment and increased transparency in developing the capacity of multinational projects and programmes (Ibid.). This shows that political-strategic cooperation is also crucial in building trust and ensuring mutual transparency.

**Countering hybrid threats**

Both organizations focused their first activities on actively involving the EU in the planning of CMX 17, which aimed to test the sustainability of jointly agreed measures on hybrid threats. The Hybrid CoE, the EU Hybrid Fusion Cell, and the NATO Hybrid Analysis cell have now been established. The newly formed entities represent the first step towards a better overview of the joint situational picture, especially since cooperation between Stratcom groups was also established at the same time. The organizations paid special attention to active communication between the two military staffs in the Stratcom area, especially in the areas of media and disinformation, exchange of analyses, and capacity development (1 - 5 Progress Report on the Implementation of the Common Set of Proposals endorsed by NATO and EU Councils on 6 December 2016/2017, NATO/EU).

At the end of 2017 the Hybrid CoE reached operational capacity, which in turn led to active cooperation between the Hybrid CoE, the EU Hybrid Fusion Cell, and the newly formed NATO Hybrid Analysis cell, as well as between the EU's Single Intelligence Analysis Capacity and NATO's Joint Intelligence and Security Division. The Battlefield Information Collection and Exploitation System (BICES)[10] network has also been set up between the EU and NATO. As a result of this cooperation, the first parallel and coordinated report was produced, and is still being produced in the same way today. The need for active cooperation between the two organizations in this field was also confirmed, as this ensures that the implication of hybrid threats is coherently addressed in the CDP and the NDPP (Ibid.).

Following the active participation of these entities, a review of cooperation in the areas of early warning and situational awareness, Stratcom and communication, crisis response, cyber defence, energy security, resilience and deterrence was carried out. The first step in the fight against terrorism was also taken, when NATO was invited to participate in Europol meetings (Ibid.).

Nevertheless, in the author’s view, the NATO Cyber Operations Centre is currently lacking in the fight against hybrid threats. Cyberspace can be used as a key tool to achieve an adversary’s goal, whether political, economic, or military, and hybrid threats can be carried out in or through cyberspace.

[10] *BICES is a multinational intelligence system that provides intelligence to NATO and its Member States (Tolga, B., I.; Faith-Ell, G., 2020, p 30).*

### Cybersecurity and defence

In the area of cybersecurity and defence, the following measures were taken: the implementation of the NCIRC/CERT-EU technical agreement; cooperation in the exchange of concepts, threat indicators, ad hoc exchange of threat warnings, and threat assessments; closer cooperation between response groups; and cross-cutting meetings focused on crisis management, cyber diplomacy, the EU cyber diplomacy toolbox, and NATO's cyber defence efforts. A EU-NATO consultation meeting was also held to discuss the NATO Cyber Defence Pledge, the EU Joint Report on Resilience, Deterrence and Defence, and the presentation of key EU cyber defence capability development projects. The main objectives of these measures were to avoid duplication of defence capacity, and it was also agreed that the Malware Information Sharing Platform (MISP) would become an operational tool for the two organizations to exchange information on cyber incidents (1 - 5 Progress Report on the Implementation of the Common Set of Proposals endorsed by NATO and EU Councils on 6 December 2016/2017, NATO/EU).

### Defence capabilities

In this area, the two military staffs conducted a review on the CPD and the NDPP to ensure coherence between the two plans and to avoid duplication of defence capabilities. It has been highlighted that the Member States have only one set of their own (national) military forces, and military staff should strive to ensure coherence between the two planning processes, so the military staff agreed that regular contacts and information exchange should become the norm to avoid duplication of existing capabilities (Ibid.). This approach confirms the stated objective of the complementarity of defence capabilities and the rationalization of resources set out in the Joint Declaration.

### Education, training, and exercises

The organizations have also made progress in the area of education, training, and exercises. Education and training was mainly focused on strengthening complementarity and exchanging best practice, with the NATO Hybrid CoE and CCDCOE being the most involved. Education took place mainly in the form of workshops, while training took place mainly in the form of exercises. The CMX exercise, which successfully completed the PACE concept, stands out, as it has proved to be a key element of EU-NATO cooperation in strengthening resilience to and combating hybrid threats. Specifically, the purpose of this concept and exercise was to achieve cooperation in four areas: early warning/situational awareness, Stratcom, cyber defence, and crisis prevention and response (1 - 5 Progress Report on the Implementation of the Common Set of Proposals endorsed by NATO and EU Councils on 6 December 2016/2017, NATO/EU).

Cooperation in cybersecurity and defence exercises has also been strengthened. The EU has joined the NATO Trident Juncture; Trident Jaguar; the Cyber Coalition, and the Coalition Warrior Interoperability Exercise, and NATO took part in the

MILEX exercise (Ibid.). These exercises do not only serve as training, but also for the exchange of experience and practical knowledge. They are a priceless source of practical knowledge and experience, and at the same time the best way to test tools and documents in place.

**Defence capacity building, the defence industry, and research**

In the area of the defence industry and research, the EU and NATO have set up a mechanism to develop a dialogue on industrial aspects, focusing on specific areas of common interest such as small and medium-sized enterprises (SMEs). Recent dialogue in this area has intensified, especially on supply chain and innovation issues, with a focus on ICT. This enhanced dialogue led to the presentation of the EU Cyber Security and Defence Package within the European Defence Fund, and NATO introduced the MISP (1 - 5 Progress Report on the Implementation of the Common Set of Proposals endorsed by NATO and EU Councils on 6 December 2016/2017, NATO/EU).

Bilateral consultations have also been held between NATO Allies and EU members, and between NATO partners and EU partners, and the adoption of common standards has been agreed, for which the Material Standardization Harmonization Team is responsible. Maintaining regular contacts between the military headquarters has prevented unnecessary duplication of international projects and initiatives, resulting in the coordination of 38 of 47 PESCO[11] projects with NATO (Ibid.).

Some measures have also been implemented in the field of innovation, especially in energy and artificial intelligence. Data exchange has been established between the EDA and the NATO Innovation Hub, and between the NATO Science and Technology Organization (STO), the European Commission, and the EDA (Ibid.).

## 3 CHALLENGES OF THE EU-NATO PARTNERSHIP: COMMON TERMINOLOGIES

Although both organizations emphasize the importance of a common and unified approach in responding to contemporary security threats, we note that the organizations do not use uniform terminology. The importance of terminology in the contemporary security environment was pointed out by Futter et al., who argue that there are no uniform definitions and understanding, especially with regard to security in cyberspace (2018, p 201; Schatz, D et al., 2017, pp 53-54). Noor took the same view, pointing out that even if we all speak the same language, we do not all

[11] *PESCO - Permanent Structured Cooperation. Under PESCO, two of the 17 flagship projects related to cybersecurity are: 1. the EU Malware Information Sharing Platform (MISP) and 2. the EU Cyber Rapid Reaction Team (CRRT) (EEAS, ESDC/Cyber Platform: Inauguration Ceremony, EEAS, 2018). The first CRRT was prepared under the lead of the Netherlands in 2019. In March 2020, six Lithuanian-led countries signed a memorandum on the CRRT, by which Lithuania, Estonia, Croatia, Poland, the Netherlands, and Romania agreed on mechanisms of operation, legal status, role, and procedures (Cyber Rapid Response Team established by six EU countries, the Lithuania Tribune, 2020).*

understand terminology equally (Noor, 2021, Tallinn Winter School in Diplomacy, e-source).

At the same time, there are also language barriers, where the meaning and understanding of a term may be lost in translation. In addition to the already known international legal gaps (e.g. the application of international law, norms, measures, etc.), therefore, the common understanding of terminology presents an additional challenge to a common and unified approach to facing the global challenges of the two organizations.

In reviewing EU and NATO documents from the cyber defence perspective, we analyzed the Allied Joint Doctrine for Cyberspace Operations (AJP-3.20. Conduct of Operations - AJP-3, edition C, version 1) and the European Union Agency for Cybersecurity (ENISA) documents, as the main organization of EU cybersecurity. In the comparisons, we focused only on the essential terms that form the basis for a unified approach in the contemporary security environment.

### Information environment

The information environment is not defined in EU documents, although this term is mentioned in some of them. Although the EDA commissioned the implementation of the EU Capability Development Analysis Plan until 2035, highlighting the importance

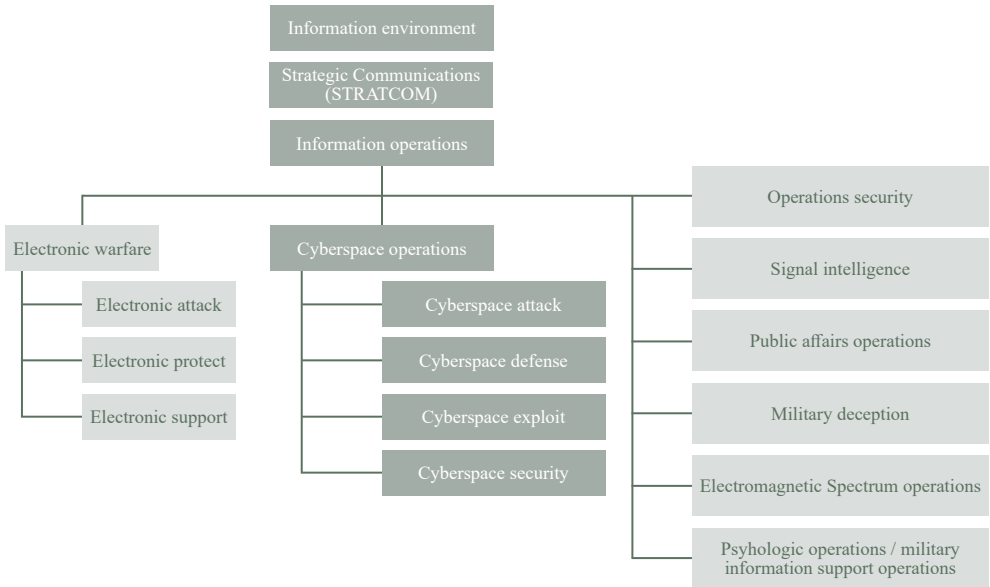



Figure 3: Information environment and forms of operation (Source: Adapted from Orye, E and Maennel, M O, 2019, p 106[12])

[12] *Until November 2012, the term Computer Network Operations was used instead of the term cyber operation. The following terms were also changed: Computer Network Attack, Computer Network Defence and Computer Network Exploit (Glossary, NIST, 2021, e-source).*

of understanding the information environment (Kepe et al., 2018, p 22), the definition itself could not be found. Within NATO documents this term is identified in AJP-3: "*A composite of the information itself, the individuals, organizations and systems that receive, process and convey the information, and the cognitive, virtual and physical space in which this occurs*," (AJP-3, p LEX-6).

This raises the question of how the EU understands the information environment, which in general terms represents the interaction between social networks and cyberspace. This issue is very important from the point of view of combating hybrid threats, as by sharing a common understanding of the information environment, organizations can develop more effective resilience to hybrid threats.

**Cyberspace**

Understanding cyberspace is as important as understanding the information environment, especially in terms of international law and the exercise of sovereign power by states. For comparison, we looked at the definition of ISO 27023, which defines cyberspace "*as a complex environment resulting from the interaction of people, software and services on the Internet, supported by worldwide distributed physical information and ICT devices and connected networks*" (ISO/IEC 27032, 2018, p VI).

ENISA defines cyberspace somewhat differently. Its definition encompasses all three layers of cyberspace: "*the time-dependent set of tangible and intangible assets which store and/or transfer electronic information*" (ENISA overview of cybersecurity and related terminology, ENISA, 2017, p 6).

NATO defines cyberspace similarly to most experts and the International Telecommunication Union (Probert, 2019, p 69), and has identified two definitions:

- Cyberspace is "*the global domain consisting of all interconnected communication, information technology and other electronic systems, networks and their data, including those which are separated or independent, which process, store or transmit data*" (NATO, AJP-3.20, p 4).
- "*Cyberspace is the virtual, non-physical domain formed by all information technology systems interconnected on a global scale*" (NATO, AJP-3, p C-3).

Thus, we are again faced with the same problem in defining the information environment, specifically in how organizations understand cyberspace. Different understanding of cyberspace influences the formulation of other definitions concerning the cyber domain, and thus the building of resistance to cyber threats, or cyber operations.

## Information Security

The NATO definition of information security is not covered in any of the aforementioned documents, but is covered by the NATO Security Directive of the Joint Operations Command and in the Security document within NATO. Instead of the term "information security", NATO uses the abbreviation "INFOSEC" and the term Information Assurance, which means the protection of all information inside/outside[1] information systems and networks, including other forms of security: physical, documentary, communication, computer, industrial, physical and security of operations (ACO Security Directive, 2012; Security within NATO, NATO, 2020). The EU´s information security is defined in different way, as ENISA states that information security is a classic information security model that defines three objectives: confidentiality, integrity and availability (ENISA overview of cybersecurity and related terminology, p 6). NATO has a similar definition, but instead of information security the term CIS (Communication and Information System) security is used, which is "*the application of security measures for the protection of communication, information and other electronic systems, and the information that is stored, processed or transmitted in these systems concerning confidentiality, integrity, availability, authentication and non-repudiation*" (Security within the NATO, NATO, 2020); this follows the ISO 27000 definition of a standard (ISO/IEC 27000, 2018, p 12). This type of definition is also defended by Longley et al. (1992, p 268), from which we can logically conclude that cybersecurity is a subset of information security. However, ENISA has taken a different definition, namely that information security and network and information systems are subsets of cybersecurity and related terminology (ENISA, 2017, p 6).

## Cybersecurity

The definitions of the two organizations also differ in defining cybersecurity. ENISA uses two definitions of cybersecurity in one document:

1. "Comprises all activities necessary to protect cyberspace, its users, and impacted persons from cyber threats";
2. "Covers all aspects of prevention, forecasting; tolerance; detection; mitigation, removal, analysis and investigation of cyber incidents".

Considering the different types of cyberspace components, cybersecurity should therefore cover the following attributes: "availability, reliability, safety, confidentiality, integrity, maintainability (for tangible systems, information and networks), robustness, survivability, resilience (to support the dynamicity of the cyberspace), accountability, authenticity and non-repudiation (to support information security)" (ENISA Overview of Cybersecurity and Related Terminology, 2017, p 6).

[1] *Includes physical and digital information.*

NATO defines cybersecurity in a much simpler way, namely as "the application for the protection of communication, information, and other electronic systems, and the information that is stored, processed or transmitted in these systems with respect to confidentiality, integrity, availability, authentication and non-repudiation" (NATO, AJP-3.20, p 4). However, the NATO definition does not include all layers of cyberspace, as a social (human) layer is not included.

## Conclusion

Over the past two decades, digital technology has become the backbone of modern society while society, in kind, has become simultaneously very vulnerable and resilient to modern security challenges. The information environment and cyberspace have created new security challenges and threats that cannot be tackled individually, with consequences spreading globally. These consequences may be completely non-kinetic or kinetic in nature, but may also be a combination of both, depending on the level of resistance achieved against modern threats.

The EU and NATO are aware of the contemporary security environment, which consists of all the domains of warfare, and whose hazard vectors are the same for both organizations. This awareness has been steadily strengthened for a long time, which has led to the signing of a joint declaration on a deepened strategic partnership. Both organizations have agreed that only joint efforts can lead to greater resilience to hybrid and cyber threats to the two organizations and their Member States, considering all the domains of warfare.

Both adopted agreements set clear objectives and goals for the EU-NATO Strategic Partnership, and 74 adopted measures made these goals concrete. The analysis showed that both organizations undertook the agreement with the utmost seriousness in all areas of common interest: political-strategic, operational and hybrid cooperation, cooperation in cybersecurity, development and capacity building, and industry and innovation. The pace of cooperation was found to have accelerated, with the greatest progress being made in implementing joint measures to combat hybrid threats, cybersecurity and defence, and capacity building, as the aim was not to duplicate but to complement capabilities. However, such efforts are also key to a fair sharing of the burden and the benefits and responsibilities between the organizations, or between the Member States of both organizations.

Despite a large number of implemented measures, some open questions remain, primarily concerning definitions and terminology. Terminological differences are present in all areas. The most worrying is the diametric nature of the understanding of information or cybersecurity. Such discrepancies can lead to different resilience and capacity building, both in the Member States and in organizations, and make it impossible to implement the principle of non-duplication and complementarity. Another open issue is the application of Article 5 and non-Article 5 of the North Atlantic Treaty, or Articles 42 and 43 of the Treaty on the EU and Article 222 of the Treaties on the Functioning of the EU. The latter issue is of an international legal nature, but the organization could also act in this area, which would provide insight

into how the Member States understand the application of international law in the case of hybrid and cyber threats.

## Bibliography

1. *ACO SECURITY DIRECTIVE, AD 70-1 (2012). Belgium: Supreme Headquarters Allied Powers Europe.*
2. *Allied Joint Doctrine for Cyberspace Operations – AJP-3.20, 2020, NATO. NSO.*
3. *Allied Joint Doctrine for the Conduct of Operations – AJP-3, Edition C, Version 1., 2019. NATO. NATO Standardization Office.*
4. *Cohen, R., 2008. Cooperative Security: New Horizons for International Order. Garmisch-Partenkirchen: George C. Marshall Center.*
5. *Council Conclusions on the Implementation of the Joint Declaration by the President of the European Council, the President of the European Commission and the Secretary General of the North Atlantic Treaty Organization. EU, 2016. https://data.consilium.europa.eu/doc/document/ST-15283-2016-INIT/en/pdf, 23. 12. 2020.*
6. *Council Conclusions on the Implementation of the Joint Declaration, 2017. EU. https://www.consilium.europa.eu/media/31947/st14802en17.pdf, 18. 12. 2020.*
7. *Cyber Defence, 2020. EDA. https://www.eda.europa.eu/what-we-do/activities/activities-search/cyber-defence, 23. 12. 2020.*
8. *Cyber Rapid Response Team established by six EU countries, 2020. The Lithuania Tribune. https://lithuaniatribune.com/cyber-rapid-response-team/, 19. 12. 2020.*
9. *Defining Computer Security Incident Response Teams. US-CERT. https://www.us-cert.gov/bsi/articles/best-practices/incident-management/defining-computer-security-incident-response-teams, 22. 2. 2021.*
10. *EEAS, ESDC: Cyber platform for education, training, evaluation and exercise (ETEE), 2018. https://www.eda.europa.eu/info-hub/press-centre/latest-news/2018/11/20/cyber-education-training-exercise-and-evaluation-(etee)-platform-launched, 19. 12. 2020.*
11. *ENISA overview of cybersecurity and related terminology. European Union Agency for Cybersecurity, 2017. https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology, 13. 2. 2021.*
12. *EU and NATO increase information sharing on cyber incidents, 2016. EEAS. https://eeas.europa.eu/headquarters/headquarters-homepage/5254_en, 23. 12. 2020.*
13. *Fourth Progress Report on the Implementation of the Common Set of Proposals endorsed by NATO and EU Councils on 6 December 2016 and 5 December 2017, 2019. NATO https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_06/190617-4th-Joint-progress-report-EU-NATO-eng.pdf, 18. 12. 2020.*
14. *Fifth Progress Report on the Implementation of the Common Set of Proposals endorsed by NATO and EU Councils on 6 December 2016 and 5 December 2017, 2020. EU. https://www.consilium.europa.eu/media/44445/200616-progress-report-nr5-eu-nato-eng.pdf, 18. 12. 2020.*
15. *Futter, A., 2018. Journal of Cyber Policy: 'Cyber' semantics: why we should retire the latest buzzword in security studies, Vol. 3, No.2. Taylor & Francis Group, pp 201–206.*
16. *Kepe, M., Black, J., Melling, J., Plumridge, J., 2018. Exploring Europe's capability requirements for 2035 and beyond: insights from the 2018 update of the long-term strand of the Capability Development Plan. Brussels: EDA.*
17. *Glossary, NIST, https://csrc.nist.gov/glossary/term/computer_network_operations, 21. 1. 2021.*
18. *Herrmann, S., D., 2001. A Practical Guide to Security Engineering and Information Assurance. New York: Auerbach Publications.*
19. *International Standard ISO/IEC27000, 2018. Geneva: ISO.*

20. *International Standard ISO/IEC27032, 2018. Geneva: ISO.*
21. *Joint Declaration on EU-NATO Cooperation, 2016. EU. https://www.consilium.europa.eu/media/24293/signed-copy-nato-eu-declaration-8-july-en.pdf, 23. 12. 2020.*
22. *Joint Declaration on EU-NATO Cooperation, 2018. NATO. https://www.nato.int/cps/en/natohq/official_texts_156626.htm, 23. 12. 2020.*
23. *LePage, R., 2014. Understanding NATO Strategic Communications. Sofia: Crisis Management and Disaster Response Centre of Excellence.*
24. *Lété, B., Pernik, P., 2017. EU-NATO Cybersecurity and Defense Cooperation: From Common Threats to Common Solutions. Policy Brief, No. 38. Washington DC: The German Marshall Fund of the United States.*
25. *Latici, T., 2020. Understanding EU-NATO cooperation: theory and practice. Brussels: European Parliamentary Research Service.*
26. *Lisbon Summit Declaration. NATO, 2010. https://www.nato.int/cps/en/natolive/official_texts_68828.htm, 21. 12. 2020.*
27. *Longley, D., Shain, M., Caelli, W., 1992. Information Security: Dictionary of Concepts, Standards and Terms. New York: Stockton Press.*
28. *Mogherini, Rehrl, 2018. Handbook on Cybersecurity: The Common Security and Defence Policy of the European Union, p 6. Vienna: Federal Ministry of Defence of the Republic of Austria.*
29. *Noor, E., Tallinn Winter School of Cyber Diplomacy, 2021. Ministry of Foreign Affairs of Estonia. https://www.youtube.com/watch?v=bxWGc4Db7Z4, 10. 2. 2021.*
30. *Orye, E., Maennel, M. O., 2019. Recommendations for Enhancing the Results of Cyber Effects, 11th International Conference on Cyber Conflict: Silent Battle NATO Cooperative Cyber Centre of Excellence, Tallinn: CCDCOE.*
31. *Pernik, P., 2014. Improving Cyber Security: NATO and the EU. Tallinn: International Centre for Defence Studies.*
32. *Pissanidis, N., Rõigas, H., Veenendaal, M., 2016. 8th International Conference on Cyber Conflict: Cyber Power. Tallinn: NATO CCD COE Publication.*
33. *Pogodba o Evropski uniji, Evropska unija, UL C 202/38, 7. 6. 2016.*
34. *Pogodba o delovanju Evropske unije, Evropska unija, UL C 202/1, 7. 6. 2016.*
35. *Probert, E. D., 2019. Organisational Structures & Incident Management for Cybersecurity in the America. ITU: SlideShare.*
36. *Progress Report on the Implementation of the Common Set of Proposals endorsed by NATO and EU Councils on 6 December 2016, 2017. NATO. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_06/20170619_170614-Joint-progress-report-EU-NATO-EN.pdf, 18. 12. 2020.*
37. *Raik, K., Järvenpää, P., 2017. A New Era of EU-NATO Cooperation: How to Make the Best of a Marriage of Necessity. Tallinn: International Centre for Defence and Security.*
38. *Relations with the European Union, 2020. NATO. https://www.nato.int/cps/en/natohq/topics_49217.htm, 18. 12. 2020.*
39. *Schatz, D., Bashroush, R., Wall, J., 2017. Journal of Digital Forensics, Security and Law: Towards a More Representative Definition of Cyber Security, Volume 12, No. 2, Florida: Embry-Riddle Aeronautic University, pp 53−74.*
40. *Second Progress Report on the Implementation of the Common Set of Proposals endorsed by NATO and EU Councils on 6 December 2016, 2017. NATO. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_11/171129-2nd-Joint-progress-report-EU-NATO-eng.pdf, 18. 12. 2020.*
41. *Security within NATO, C-M(2002)49-REV1, 2020. NATO.*
42. *Svete, U., 2005. Varnost v informacijski družbi. Ljubljana: Fakulteta za uporabne družbene študije.*

43. *Svete, U., 2007. Varnostne implikacije uporabe informacijsko-komunikacijske tehnologije. V: Elektronsko upravljanje in poslovanje v službi uporabnika / Pintarič, U. (ur.). Ljubljana: Fakulteta za družbene vede, pp 160–161.*
44. *Statement on the Implementation of the Joint Declaration signed by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization, 2016. https://www.nato.int/cps/en/natohq/official_texts_138829.htm, 18. 12. 2020.*
45. *Third Progress Report on the Implementation of the Common Set of Proposals endorsed by NATO and EU Councils on 6 December 2016 and 5 December 2017, 2018. EU. https://www.consilium.europa.eu/media/35578/third-report-ue-nato-layout-en.pdf, 18. 12. 2020.*
46. *Tolga, B., I., Faith-Ell, G., 2020. Information Sharing Framework for Penetration Testing. Tallinn: CCDCOE.*
47. *The Brussels Treaty. NATO. https://www.nato.int/cps/en/natohq/official_texts_17072.htm, 19. 12. 2020.*
48. *Zakon o kritični infrastrukturi (ZKI). (Critical Infrastructure Act) Official Gazette of the Republic of Slovenia, No 75/17 of 22 December 2017.*