Finabel

Food for thought 11-2021

Defending The EU Against Cyber Operations

Mechanisms, Challenges And Cooperation With NATO

AN EXPERTISE FORUM CONTRIBUTING TO EUROPEAN ARMIES INTEROPERABILITY SINCE 1953

FINABEL
European Army Interoperability Centre

Written by
Luca Vignati, Euan Scott,
Krastina Razheva, Jorida Vela

This Food for Thought paper is a document that gives an initial reflection on the theme. The content is not reflecting the positions of the member states but consists of elements that can initiate and feed the discussions and analyses in the domain of the theme. All our studies are available on www.finabel.org

DIRECTOR'S EDITORIAL

In the past few years, the EU has faced serious challenges and threats occurring in its cyberspace. A number of Member States have been targeted by malicious cyber operations and intrusions, with some large-scale cases, such as the Russian cyber-attacks against Estonia in 2007. These operations represent a serious political, economic, and military threat for the individual Member States and the EU as a whole – and for this reason, the EU has turned its attention to the issue to strengthen its framework for counteraction of cybercrime. So far, this resulted in the adoption of the first Cyber Security Strategy in 2013 and the renaming of the European Network and Information Security Agency (ENISA) as the European Union Agency for Cybersecurity in 2019, with a new permanent mandate established by the EU Regulation 2019/881, highlighting the growing importance of protecting the EU's cyberspace.

Cybercrime is perceived as a serious threat not only for the EU, but also for NATO. Therefore, NATO is simultaneously developing its cybersecurity strategies, beginning with establishing a Cyber Defence Policy in 2008. Since both organisations recognise cybersecurity as a key challenge to their core objectives and many of the EU Member States are also part of NATO, it is only logical that an effective and efficient cybersecurity strategy would include cooperation between the organisations. This cooperation became evident as of 2016 when the EU and NATO signed a Technical Arrangement on Cyber Defence, aiming to establish common cybercrime detection and response mechanisms. This common strategy is still facing a number of issues, including a lack of information sharing but is undoubtedly a vital step towards the harmonisation of cyber defence.

Mutual efforts of the EU and NATO on security matters are a point of high significance for FINABEL. And even though cybersecurity as a concept is not developed to as large an extent as the protection of a State's physical integrity, it is a notion that will become increasingly relevant, especially considering ever-growing digitalisation and the use of computer technologies in essentially all State-related matters. For this reason, it is important and thought-provoking to analyse the individual cybersecurity strategies of the EU and NATO and their collective efforts to counteract cybercrime, from both a theoretical and a practical perspective.

Mario Blokken
Director PSec

TABLE OF CONTENTS

ACRONYMS

CEC	Central Election Commission
CG	Cooperation Group
CSIRTs	Computer Security Incident Response Teams
CSSs	Cyber Security Strategies
DDoS	Denial of Service
EEAS	European External Action Service
EC	European Commission
EP	European Parliament
ENISA	European Network and Information Security Agency
EU	European Union
EU-CyCLONe	European Cyber Crises Liaison Organisation Network
IPCR	Integrated Political Crisis Response
MS	Member States
NIS	Security of Network and Information Systems
NATO	North Atlantic Treaty Organisation
NATO CCCDE	NATO Cooperative Cyber Defence Centre of Excellence
JCU	Joint Cyber Unit
SCADA	Supervisory Control and Data Acquisition network
TF-CSIRT	Task Force on Computer Security Incident Response Teams

INTRODUCTION

The modern world is witnessing digitalisation at an extraordinary pace. Computer systems are being implemented in almost all forms of human activity to improve the accuracy and efficiency of processes and to facilitate daily life overall. Likewise, digital technologies are present in many State-related matters, from providing services in the public sector to government administration and State security. At this point, it may safely be asserted that the functioning of a particular State and its institutions is dependent on digital technologies. For this reason, it is of the utmost significance to ensure that the relevant computer systems are secure and stable, the practice known as cybersecurity.

Even though introducing digital technologies to State matters undoubtedly brings about many benefits, it also presents a system that is very susceptible to interference from malicious counterparties. The unlawful interference with computer systems, called cybercrime, is an increasingly large threat to State security. Large-scale cyber-attacks on State structures have already occurred, demonstrating their destructive potential. Therefore, it is of the utmost significance that adequate levels of cybersecurity and resilience are ensured on a national level. To achieve this, States need to act both from a legal perspective – implementing relevant legislation pertaining to cybersecurity – and from a practical perspective – putting in place mechanisms for the timely detection and neutralisation of cyber threats.

Source: Stockvault, https://www.stockvault.net/photo/252628/gdpr-business-laptop

GDPR Business Laptop

Without a doubt, cybercrime is a threat not only on a national level, but also on an international level. It is recognised by both the EU and NATO as one of the greatest challenges to their security policies and, thus, an element that needs to be adequately secured. For this reason, both organisations are developing extensive cybersecurity agendas that will allow them to assess and counteract cybercrime within their Member States and collaborate with one another.

The following Food for Thought paper will conduct an in-depth analysis of how the EU and NATO ensure cybersecurity. It will begin with Chapter 1, delineating what precisely constitutes cybercrime and the different categories of cyber threats. Furthermore, the cybersecurity strategy of the EU will be laid out, examining all relevant legislation and the various strategies established within the EU. Special regard will be paid to the European Union Agency for Cybersecurity and the Joint Cyber Unit – two of the milestones of the EU cybersecurity policy. Following this, Chapter 2 will depict cybercrime from a practical perspective, focusing on two of the most large-scale incidents to date – namely, the 2007 attacks on the Estonian government and the 2014 attacks on Ukraine. This chapter will also demonstrate the practical implication of the EU's cybersecurity policy. Finally, Chapter 3 will discuss the cybersecurity strategy of NATO and the joint efforts of NATO and the EU to fight cybercrime, focusing on a number of collaborative projects aiming to secure the cybersphere within the two organisations. The paper will conclude with an assessment of the importance of cybersecurity as related to the topics already discussed, and a brief insight into the future of the field.

THE EVOLUTION OF THE EUROPEAN UNION STRATEGY ON CYBERSECURITY

Definition and Categories of Cyber Threats

The security of the cybersphere, both on a national and international level, has always been threatened by the actions and crimes committed by malicious cyber operators. The sophistication and the potential pervasiveness of their cyber threats have attracted the attention of various States and international organisations, including the European Union (EU) and NATO, prompting further cooperation and the provision of effective legal instruments for the protection of cyberspace and its users.[1]

"Cyber threats" can be labelled as acts of destruction of computer networks or data contained therein through interference or interception. They are characterised by the use of computers and by the fact that their target is a computer network or part of it.[2] Cyber threats can be divided into three categories: cyber

[1] Nureni Ayofe Azeez and Barry Irwin, 'Cybersecurity: Challenges and the Way Forward', Computer Science & Telecommunications 29, no. 6 (2010). [online] Available at: https://www.researchgate.net/publication/265121167_CYBER_SECURITY_CHALLENGES_AND_THE_WAY_FORWARD_

[2] Aaron J. Burstein, 'Towards a culture of cybersecurity research'. [online] Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1113014

threats against individuals, against properties, and governments.

Cyber threats against individuals include several criminal acts, such as cyber harassment, including acts of harassment based on racial, religious, or sexual grounds. One of the major international crimes included in this category is the diffusion and distribution of child pornography, along with other kinds of prohibited material. Another major cyber threat in this category is the violation of privacy.[3] Cyber threats against properties include the diffusion of unlawful and harmful cyber programmes and the stealing of relevant technical knowledge and other sensitive material from private companies, often in the context of industrial espionage. Lastly, cyber threats against governments include cyberterrorism, which has seen a relevant increase in the last years, with individuals and terrorist organisations using the internet to threaten both governments and citizens, and as a means of support for their activities.

More specifically, among the most prevalent cyber threats are hacking, computer fraud, phishing, spamming, denial of service attacks, and other forms of viruses, which are mostly committed for economic reasons, to make threats, and to gain recognition for the actors committing them.[4] Therefore, various States and international organisations have engaged in developing relevant legislation and mechanisms to adequately prevent and confront these acts. The EU has progressively placed more attention on this field but faces the additional challenge of different definitions of cyber threats between its Member States (MS).

Strategies and Directives for Cybersecurity

During the 1990s, various European countries formed national Computer Security Incident Response Teams (CSIRTs). European coordination regarding cybersecurity became evident at the end of the decade with the formation of a trans-national "cyber-security community". This community initially relied on informal relationships between its members, who supported each other and shared information in a *quid pro quo* fashion.[5] A more structured network, the Task Force on Computer Security Incident Response Teams (TF-CSIRT), which still relied on the voluntary participation of its members, was formed in 2000 and served as a forum dedicated to the exchange of experience and knowledge and promoting collaboration and coordination between the different national CSIRTs, while assisting in the development of common standards and procedures and organising joint initiatives.[6]

The network's informality progressively showed its flaws during the 2000s, culminating with the 2007 cybersecurity attacks sustained by the Internet infrastructure of Estonia.[7] At the same time, the EU provided new instruments with a stronger legal basis. By 2004, the EU, with Regulation 460/2004, created the European Network and Information Security Agency (ENISA). ENISA's

[3] Herbert Lin et alia, 'Towards a Safer and More Secure Cyberspace'. [online] Available at: https://www.researchgate.net/publication/220426062_Toward_a_safer_and_more_secure_cyberspace

[4] Id.

[5] Kas Clark et al., "A Dutch Approach to Cybersecurity Through Participation", IEEE Security & Privacy 12, no. 5 (September 2014): 29.

[6] Géant, 'TF-CSIRT: Computer Security Incident Response Teams'. [online] Available at: https://www.geant.org/People/Community_Programme/Task_Forces/Pages/TF-CSIRT.aspx

[7] Ruohonen et al., "An Outlook on the Institutional Evolution of the European Union Cyber Security Apparatus": 749.

main task, in its original form, was collecting information, providing the various European institutions and the MS with advice on network and information security problems, enhancing the cooperation between the different actors operating across different fields, such as the fields of industry or Academia, and facilitating the cooperation between the European Commission (EC) and the MS in the development of common methodologies.[8]

This move towards a more developed and organised European strategy for preventing and countering cyber-attacks and incidents was further strengthened with the establishment of common Cyber Security Strategies (CSSs). The first CSS was announced in February 2013. The EU also undertook other steps to counter cyber-related crimes and established, for example, the European Cybercrime Centre in collaboration with the European Police Office in January 2013.[9] The proposed EU security strategy is founded on five fundamental priorities: achieving cyber resilience, drastically reducing cybercrime, developing cyber defence policy and capabilities related to the Common Security and Defence Policy (CSDP), developing the industrial and technological resources for cyber-security, establishing a coherent international cyberspace policy for the EU, and promoting its core values.[10] The CSS highlights the importance of the collaboration between the public authorities and the private sector, along with the improvement of the prevention, detection, and management of cyber-attacks through coordination at the EU level – with a stronger role for ENISA.[11]

At the legislative level, one of the most important features envisaged by the CSS is Directive 2016/1148 on Security of Network and Information Systems (NIS Directive), adopted by the European Parliament (EP) in July 2016, which entered into force in August 2016. The NIS Directive is the first piece of EU-wide legislation on cybersecurity, providing legal measures to boost the overall level of cybersecurity in the EU.[12] The Directive, which applies to operators of essential services and digital service providers, also requires that all MS have minimum capabilities and a strategy ensuring a high level of security of NIS in their countries.[13]

For this reason, the Directive requires each MS to adopt a national strategy on the security of NIS, allowing them to request the assistance of ENISA, and communicate their strategy to the EC within three months from its adoption.[14] In addition, each MS is required to designate one or more national authorities to monitor the Directive's application at the national level and a national single point of contact (which can coincide with the national authority, if the MS designates only one) acting as a liaison to ensure the cross-border cooperation of the MS.[15] Finally, the Directive establishes a network of the national CSIRTs

[8] European Parliament and Council of the European Union, "Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency", OJEU L077/2004, Art. 3(a)-(d).

[9] European Commission, 'European Cybercrime Centre (EC3) opens on 11 January'. [online] Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_13_13

[10] European Commission, 'EU Cybersecurity plan to protect open internet and online freedom and opportunity'. [online] Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_13_94

[11] László Kovács, "Cyber Security Policy and Strategy in the European Union and NATO", Land Forces Academy Review 23, no. 1 (2018): 18.

[12] European Commission, 'NIS Directive'. [online] Available at: https://digital-strategy.ec.europa.eu/en/policies/nis-directive

[13] European Parliament and Council of the European Union, "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union", OJEU L194/2016, p. 1(4)(7). The Annex II of the Directive lists as operators of essential services the entities providing services in the fields of energy, transport, banking, financial market infrastructures, health, drinking water supply and distribution, digital infrastructure.

[14] Id., Art. 7.

[15] Id., Art. 8(1)-(4).

composed of representatives of the MS and the EC, participating as observers, with ENISA providing the secretariat and actively supporting cooperation among the CSIRTs;[16] the network aims to provide a forum for the exchange of information between the CSIRTs and provides assistance and support in the event of cyber incidents, either happening within a MS territory or cross-border.[17]

More recently, in December 2020, the EC and High Representative of the Union for Foreign Affairs and Security Policy Josep Borrell presented a new CSS, titled 'EU's Cybersecurity Strategy for the Digital Decade'. This updated CSS was published during the ongoing Covid-19 pandemic, which further accelerated the process of digitalisation through, for example, an increase of telework, with 40% of workers in the EU switching to either full-time or part-time telework.[18] This increase in digitalisation implies a corresponding increase in vulnerability to cyber-attacks. On a broader, geopolitical level, tensions over the global internet are reflected in a growing number of States erecting "digital borders", threatening the openness of cyberspace and the core values of the EU: the rule of law and the fundamental rights freedom and democracy.[19] This is worsened by security concerns, which are a major disincentive to using online services – with two-fifths of EU users experiencing security-related problems and three-fifths claiming to feel unable to protect themselves against cybercrime.[20]

As pointed out by the CSS, the EU still lacks a collective situational awareness of cyber threats, owing to the reticence of MS in systematically gathering and sharing information.[21] In addition, only limited mutual operational assistance between MS is currently in place, and no operational mechanism is present between the MS and EU institutions and bodies in the event of large-scale, cross-border cyber incidents or crises.[22] Thus, the scope of action of the new CSS focuses on addressing the threats to the cybersphere, enhancing the collective response of the EU and cooperation between the MS and between the MS and the EU. The proposals of the CSS affect three areas of EU action: resilience, technological sovereignty, and leadership; building operational capacity to prevent, deter and respond; and advancing a global and open cyberspace through increased cooperation.[23]

To address the aforementioned areas of action, the CSS proposes a revision to repeal the NIS Directive; said proposal was adopted by the EC in the same month, December 2020. The revision, NIS 2 Directive, is characterised by the introduction of a new category of services, essential entities (EEs), which replaces the previous categories of operators of essential services and digital service providers, and includes new sectors, such as telecommunications, chemicals, postal services, and public administration.[24] This broadening of the types

[16] Id., Art. 12(2).
[17] Id., Art. 12(3)(a-e).
[18] European Commission and High Representative of the Union for Foreign Affairs and Security Policy, "Joint Communication to the European Parliament and the Council – The EU's Cybersecurity Strategy for the Digital Decade", JOIN/2020/18: 1.
[19] Id.: 1-2.
[20] Id.: 2.
[21] Id.: 3.
[22] Id.: 4.
[23] European Commission, 'New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient'. [online] Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391
[24] European Commission, "Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive 2016/1148", COM/2020/823, Annex I: 1-8.

of sectors taken into account by the Directive is coupled with broadening its territorial effects compared to the previous NIS Directive. Indeed, providers of digital infrastructure (including online search engines, social networking platforms, and online marketplaces) that are not established in the EU but still offer services within the EU, are covered by the Directive and are obligated to nominate a representative to act on behalf of the provider and be at the disposal of the competent authorities and the CSIRTs.[25] Any sector which fails to comply with the provisions of the Directive shall be sanctioned by the MS with administrative fines, with a maximum amount of at least 10 million euros or up to 2% of the total worldwide annual turnover of the undertaking – depending on which of the two is higher.[26] All medium and large enterprises, as defined by Commission Recommendation 2003/361/EC, that operate within the sector covered by the NIS 2 Directive fall within its scope, while the NIS Directive makes MS responsible for determining which entities meet the criteria to qualify as operators of essential services ('identification process').[27] Small and micro entities with a key role for the economies and societies of MS or particular sectors or types of services should be covered by the Directive.[28]

Source: https://www.flickr.com/photos/mastababa/43132732422

Bronze Soldier Memorial, Tallin, Estonia
Babak Fakhamzadeh

[25] Id.: 26 (65).
[26] Id.: Art. 31(4).
[27] Id.: 14 (8).
[28] Id. (9)

In view of enhancing a quick and efficient response to cyber incidents, the aforementioned entities have to report without delay to the competent authorities or national CSIRTs any cyber-related incident or threat having a significant impact on the provision of their services and the recipients of their services.[29]
On a nationwide level, each MS is required to adopt a cybersecurity strategy defining the strategic objectives, appropriate policy, and regulatory measures.[30] MS shall also designate one or more competent authorities (National Cybersecurity Crisis Management Framework) dedicated to managing large-scale cyber incidents and crises, for which they must assure adequate resources for effective and efficient performance of their duties.[31] The concept of a national point of contact designated by MS, which should coordinate with the other corresponding points of contact in response to cross-border cyber incidents, remains in the NIS 2 Directive.[32]

Enhancing cooperation is essential for better management of cyber incidents, especially when they have a cross-border character. At the national level, the competent authorities, the national points of contact and the CSIRT of the same MS are required to cooperate concerning fulfilling the obligations contained in the Directive.[33] At the supra-national level, the NIS 2 Directive establishes the Cooperation Group (CG), whose scope is to support and facilitate strategic cooperation and exchange of information among MS in the fields covered by the Directive.[34] The CG shall be composed of representatives of the MS, the EC (which provides its secretariat), and ENISA, with the European External Action Service (EEAS) able to participate as an observer and, when appropriate, with invited representatives of relevant stakeholders as participants.[35] The CG is vested by the Directive with various tasks, such as providing guidance to the national authorities in relation to the transposition and implementation of the Directive; exchanging best practices and information related to the fields covered by the Directive between the MS, the EC, and other relevant EU institutions; providing strategic guidance to the CSIRTs network; facilitating the exchange of national officials through a capacity-building programme; and discussing the work undertaken in relation to cybersecurity exercises, including the work done by ENISA.[36]

Additionally, the Directive establishes the European Cyber Crisis Liaison Organisation Network (EU – CyCLONe), whose objective is to enable cooperation in managing large-scale cybersecurity incidents and crises, while at the same time ensuring a regular exchange of information among the MS and the EU institutions.[37] EU-CyCLONe shall be composed of representatives of the MS crisis management authorities, the EC, and ENISA, which provides the secretariat. The tasks of EU-CyCLONe are to increase the level of preparedness for managing large-scale inci-

[29] Id.: Art. 20(1). An incident is deemed as "significant" if it has caused or has the potential to cause substantial operational disruption or financial losses for the entity; or if it has affected of has the potential to affect other natural or legal persons by causing considerable material or non-material losses – Art. 20(3).
[30] Id.: Art. 5(1).
[31] Id.: Art. 7(1).
[32] Id.: Art. 8(3)(4).
[33] Id.: Art. 11(1).
[34] Id.: Art. 12(1).
[35] Id.: Art. 12(3).
[36] Id.: Art. 12(4).
[37] Id.: Art. 14(1).

dents and crises, develop a shared situational awareness of relevant cybersecurity events, coordinate the management of large-scale incidents and crises, and discuss national cybersecurity incident and response plans.[38] To fulfil its tasks, EU-CyCLONe shall cooperate with the CSIRTs network and the CG, producing regular reports on cyber threats, incidents and trends with a particular focus on their impact on essential entities.[39]

A New Role for ENISA

The aforementioned Directives, along with the other innovative features, present a strengthened role for ENISA. This new position for the Agency should be read in accordance with another important EU legislative document relating to the work of ENISA: Regulation 2019/881 (Cybersecurity Act), approved by the EP and the Council in April 2019. The Regulation replaces an older legislative document on the matter, Regulation 526/2013, and gives additional powers to ENISA. The new mandate of ENISA is highlighted by the change of its name. Although retaining its original acronym, the Agency changes its name to the European Union Agency for Cybersecurity, emphasising the importance of achieving a high level of cybersecurity and cyber resilience within the EU.[40] In addition, its mandate, which was due to terminate in 2020, was rendered permanent.[41]

The role of ENISA before the Cybersecurity Act was mostly for technical assistance to MS. With the Act, ENISA has more substantial powers, increasing operational cooperation at the EU level.[42] In particular, ENISA is vested with the task to assist with the implementation of EU policy and law relating to cybersecurity, in particular relating to the NIS Directive, through issuing opinions and guidelines and providing advice and best practices on topics such as risk management, incident reporting, and information sharing.[43] Capacity-building is considered one of ENISA's main areas of action; in this sense, the Agency shall assist MS and EU institutions in their efforts to prevent, detect, and respond to cyber threats and incidents and help with the development of national CSIRTs and strategies, both at national and EU-wide level.[44]

Promoting cooperation is considered an essential part of ENISA's work. The Cybersecurity Act explicitly affirms that ENISA shall support the operational cooperation among MS, EU institutions, and stakeholders.[45] This cooperation shall include EU institutions, the services dealing with cybercrime, and the supervisory authorities dealing with protecting privacy and personal data.[46] The cooperation with the CSIRTs Network includes ENISA's provision of its secretariat, as already noted, and the Agency's assistance to MS, including assistance relating to specific cyber threats, if requested, and analysis of vulnerabilities and incidents. In addition, ENISA shall organise regular cybersecurity exercises, including

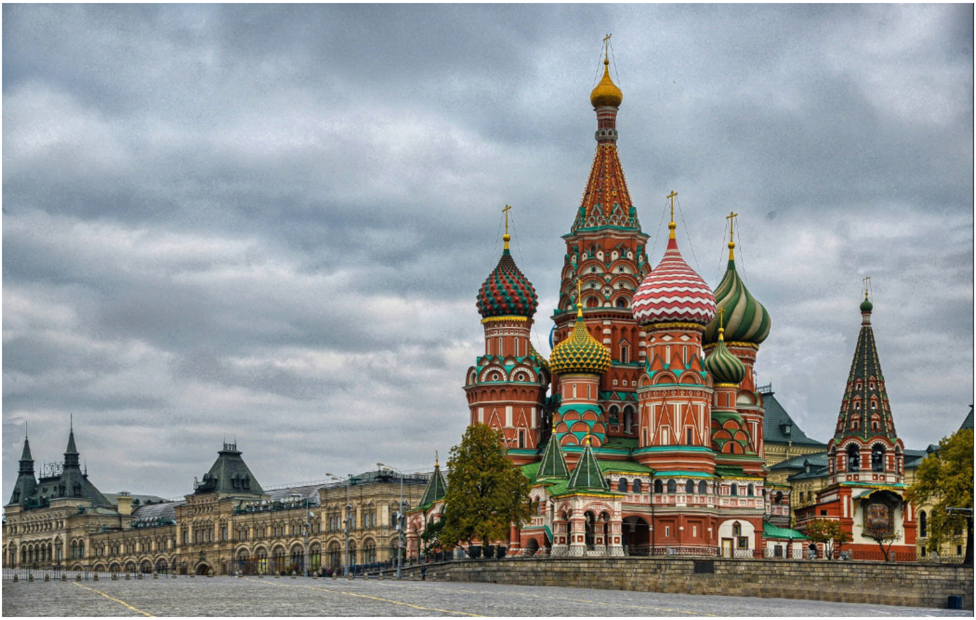
[38] Id.: Art. 14(3).
[39] Id.: Art. 14(5)(6).
[40] European Parliament and Council of the European Union, "Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)" OJEU L151/15: Art. 1.
[41] Id.: Art. 68(4).
[42] European Commission, 'The EU Cybersecurity Act'. [online] Available at: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act
[43] Art. 5(2) Regulation (EU) 2019/881.
[44] Id.: Art. 7(1)(a-e).
[45] Id.: Art. 8(1).
[46] Id.: Art. 8(2).

technical, operational or strategic elements, and prepare, in close coordination with MS, regular reports on incidents and cyber threats using all publicly available information – including information shared by the national CSIRTs and points of contact.[47]

This cooperation should also involve developing a collective response to cross-border incidents and crises, which ENISA can facilitate through other means, ensuring an efficient flow of information, escalation mechanisms, and technical handling between the MS and the EU institutions.[48] Cooperation is not limited to MS and the EU, and can also include third countries and other international organisations, as well as relevant international cooperation frameworks. ENISA can thus assist third parties at the request of the EC, for example, facilitate the exchange of best practices or provide them with expertise, and act as an observer in the organisation of international exercises, reporting their outcome to its Management Board.[49]

The Joint Cyber Unit

One of the most recent innovations proposed by the EU as part of its cybersecurity policy is the establishment of a Joint Cyber Unit (JCU). This proposal is contained in a June



Source: Stockvault, https://www.flickr.com/photos/jlascar/19345522243

The Cathedral of Vasily the Blessed, Moscow, Russia.

Jorge Láscar

[47] Id.: Art. 7(1-6).
[48] Id.: Art. 7(7).
[49] Id.: Art. 12.

2021 Recommendation by the EC and the High Representative of the Union for Foreign Affairs and Security Policy Josep Borrell, although in 2020, EC President Ursula von der Leyen already suggested developing a unit at the EU level to favour a more centralised cybersecurity approach.[50] The JCU is part of the latest EU CSS, whose aim is to ensure a global and open internet with strong safeguards, which affect three areas of EU action: resilience, technological sovereignty and leadership; operational capacity to prevent, deter and respond; and cooperation to advance a global and open cyberspace.[51]

The JCU develops the work started by the EC Recommendation 2017/1584 (called Blueprint), whose aim is to deal with large-scale cyber incidents and threats causing disruption too extensive for the concerned MS to handle on its own or affecting two or more MS or EU institutions with such a wide-ranging and significant impact of technical or political significance that they require timely policy coordination and response at the EU political level.[52] The Blueprint is characterised by the use of crisis management mechanisms, such as the Integrated Political Crisis Response (IPCR) and the ARGUS rapid alert system, which involve a large number of institutions[53] and cover a large number of fields – including health, transport, financial matters, and disaster management.

The JCU, on the other hand, is fully dedicated to cooperation in the field of cybersecurity. The Unit is set to work in close cooperation with ENISA, and with the Computer Emergency Response Team (CERT-EU), established in 2011, composed of IT security experts from the main EU institutions.[54] This close cooperation should be facilitated by the geographical location of the three organisations – the JCU and CERT-EU are established in Brussels, where ENISA, whose main headquarters are in Athens, is set to open an office.[55]

JCU aims to help civilian, law enforcement, diplomatic, and cyber defence communities in their cooperative task to prevent, deter, and respond to cyber-attacks. To reach this objective, the mandate of JCU includes various actions, such as establishing a virtual platform with tools for secure and rapid information-sharing; delivering the EU cybersecurity incident and crisis response plan (based on the national plans established by the NIS 2 Directive); establishing and mobilising EU Cybersecurity Rapid Reaction Teams; concluding memoranda of understanding and operational agreements with various actors, including private sector companies; and setting a multi-annual plan to coordinate exercises and organising joint exercise and training.[56]

For the definitive establishment of JCU, the EC has proposed a gradual building process, with four main steps, to be completed between 2021 and 2023. The first step is to assess the organisational aspects and identify

[50] Simona Autolitano, 'A Europe Fit for the Digital Age: The Quest for Cybersecurity Unpacked', Istituto Affari Internazionali [online] Available at: https://www.iai.it/en/pubblicazioni/europe-fit-digital-age-quest-cybersecurity-unpacked

[51] European Commission, 'The Cybersecurity Strategy'. [online] Available at: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

[52] Ioannis Askoxylakis, 'Blueprint - European coordinated response to large-scale cybersecurity incidents and crises', European Commission. [online] Available at: https://www.enisa.europa.eu/events/artificial-intelligence-an-opportunity-for-the-eu-cyber-crisis-management/workshop-presentations/20190603-ec-blueprint.pdf

[53] For example, the ARGUS mechanism can involve up to 42 DGs, the EEAS and other EU agencies.

[54] CERT-EU, 'About Us'. [online] Available at: https://www.cert.europa.eu/cert/plainedition/en/cert_about.html

[55] European Commission, 'Establishment of a local office presence of ENISA in Brussels, Belgium'. [online] Available at: https://digital-strategy.ec.europa.eu/en/news/establishment-local-office-presence-enisa-brussels-belgium

[56] European Commission, 'Joint Cyber Unit'. [online] Available at: https://digital-strategy.ec.europa.eu/en/policies/joint-cyber-unit

EU operational capabilities by 31 December 2021. The second is to prepare national incident and crisis response plans and introduce joint preparedness activities by 30 June 2022. The third measure is to operationalise by mobilising EU Rapid Reaction teams, following procedures defined in the EU incident and crisis response plan by 31 December 2022. The final step is to involve private sector partners, users, and providers of cybersecurity solutions and services to increase information sharing and escalate EU coordinated response to cyber threats by June 2023.[57]

Considering these developments, it may be asserted that the European Union is well underway to establish an effective, all-encompassing cybersecurity strategy very shortly. The need for this has been highlighted by the EC President Ursula von der Leyen in her State of the Union speech in front of the EU Parliament in September 2021, where she explicitly connected the issues of cybersecurity and defence and affirmed the will of the EU to become a leader in cybersecurity, stating the necessity to adopt additional instruments, such as a European Cyber Defence Policy and a new European Cyber Resilience Act.[58] However, to assess how this strategy is to be applied in practical terms, it is essential to understand precisely what a cyber-attack entails and its impact on the security and integrity of a given State. For this reason, the following chapter will present an overview of two of the most severe incidents to date – namely, the Russian cyber-attacks on Estonia and Ukraine.

CASE STUDIES OF RUSSIAN CYBER-ATTACKS

2007 Russian Cyberattacks on Estonia

April 2021 marked fifteen years since Estonia came under attack from what is known as the first-ever cyberwar. Indeed, over three weeks, banks, national ministries, governments, the media, police, the national emergency number, and even small businesses were victims of Denial of Service (DDoS) attacks that took down their websites and ICT systems.

Cyberspace's importance had only started growing in 2004 with Estonia's National Security Concept, meaning that the country lacked an overall cybersecurity strategy in 2007. This was combined with an underdeveloped international cybersecurity environment, given that cybersecurity relations between countries were still quite informal and based on a *quid pro quo* principle. In contrast, Estonia's economy heavily relied on the internet, with a 60% internet penetration ratio. As Jaan Priisalu, head of IT risk management for Swedbank AS's Estonia subsidiary in 2009, explains: "the Estonian economy was very vulnerable to an attack from cyberspace as it depended greatly on the internet. For example, 98% of bank transactions were done electronically" [59] even in 2007.

[57] Id.

[58] European Commission, '2021 State of the Union Address by President von der Leyen'. [online]. Available at: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_21_4701

[59] https://www.youtube.com/watch?v=oGZkCdpPLBE&t=34s 6'30. Jaan Priisalu.

Such a setting made Estonia a vulnerable target to events that would profoundly change cyber defence capabilities, institutions, and legislation within the country, the European Union, and NATO.

The project truly angered Russian officials. That same month, Sergei Ivanov – who was the First Deputy Prime Minister at the time, ordered Russians to spurn any product or service coming from Estonia: "Don't buy Estonian products [...], don't go to Estonia for vacations, go to Kaliningrad." [60] Even Vladimir Putin and the Foreign Minister Sergey Viktorovich Lavrov had something to say about the matter, talking about an "insult to their people, sowing discord and new distrust between states and people", [61] and a blasphemy that would have serious consequences regarding its relations with Estonia.[62]

The same day that projects for excavation began, Estonia was heavily hit with DDoS attacks, which would last for three weeks and stop abruptly on 19 May 2007 at around midnight. The attacks reached their peak on 9 May. This date is known in the Russian Federation as Victory Day, which commemorates Nazi Germany's surrender to the USSR on 9 May 1945. At the peak, the cyber-attacks took 58 governmental and corporate websites offline, including the sectors mentioned above like banking and media services, leaving the political and social spheres as well as the economy paralysed. By shutting down these electronic channels, the hackers could cut the circulation of money, information, and communication and therefore freeze the country. The Russian government denied any involvement whatsoever in these attacks. While everything pointed towards Russia, and there is no doubt about it today, the fact that this was a cyber-attack perpetrated through DDoS attacks gave Russia plausible deniability to gainsay these types of statements. The trouble is that these cyber-attacks are very hard to trace, and even if they were traced back to Russia, IP addresses could be faked. Even when NATO and Estonia managed to trace IP addresses back to Moscow, including one coming from Putin's presidential administration, officials denied such involvement, alleging the possibility for hackers to hack IP addresses even from outside of Russia and use them. In any case, the characteristics of these attacks make it highly unlikely that they were just actions perpetrated by individuals without any incentives. The high sophistication and coordination behind these attacks suggest the contrary. As Jaan Priisalu again explains, it was the fact that these DDoS attacks were so well coordinated that brought down all these services rely on the internet: "These were Service of Denial attacks where very many computers sent a lot of queries to our servers. While we usually have thousands of clients sending their queries, now there were hundreds of thousands, and they repeated their queries more frequently than people usually do." [63]

Moreover, Russian authorities failed to punish these kinds of actions within their own country, suggesting they at least encouraged

[60] Sergei Ivanov quoted in: "Here We Go Again," The Baltic Times, 4 April 2007, https://www.baltictimes.com/news/articles/17635/

[61] Vladimir Putin (translated), "Speech at the Military Parade Celebrating the 62nd Anniversary of Victory in the Great Patriotic War," Kremlin.ru, 9 May 2007, http://en.kremlin.ru/events/president/transcripts/24238

[62] "Transcript of Remarks and Replies to Media Questions by Russian Minister of Foreign Affairs Sergey Lavrov Following Ministerial Meeting of Russia-NATO Council, Oslo, April 27, 2007," The Ministry of Foreign Affairs of the Russian Federation, http://www.mid.ru/en/press_service/minister_speeches/-/asset_publisher/7OvQR5KJWVmR/content/id/375128

[63] https://www.youtube.com/watch?v=oGZkCdpPLBE&t=34s. 1'20: Jaan Priisalu.

this type of behaviour. This makes Russia, at a minimum, indirectly responsible for this cyberwar.

In contrast, other countries within the EU and organisations like NATO were there to help their fellow Member State when it called for help, despite never having faced something like this before. As Suleyman Anil, the head of NATO's Cyber Defence Support and Coordination Centre in 2009, recalls: "NATO received for the first time from a member nation an assistance request to defend against cyberattacks. So, NATO was not fully ready for it because it had never seen this before, but put a small unit of SSN, in terms of sending an observer there, who following the incidents played a harmonisation role by coordinating with the other member nations (…) to help colleagues in Estonia".[64]

The North Atlantic Treaty Organization is well known for its founding treaty's Article 5, which states that an attack on any one of the 30 allies will be considered an attack on them all. This means that if Russia had attacked through more conventional means, NATO would have used Article 5 of the Treaty. Here though, Estonia wasn't attacked through conventional means but rather through Denials of Service. These cyber-attacks were considered by NATO's Secretary-General (2004-2008) Jaan de Hoop Scheffer as a security issue: "These cyber-attacks have a security dimension without any doubt and that is the reason that NATO expertise was sent to Estonia to see what can and should be done. [...] Does this have a security implication? Yes, it does have a security implication. Is it relevant for NATO? Yes, it is relevant for NATO. It is a subject which I am afraid will stay on the political agenda in the times to come". As can be seen, triggering Article 5 was considered, but the idea was eventually discarded.

First, it wasn't possible to determine who was responsible for these attacks without conjecture, as we have seen. But most importantly, the level of gravity of DDoS attacks did not seem to warrant the activation of Article 5. Indeed, it did not seem like any critical infrastructure, such as the Supervisory Control and Data Acquisition Network (SCADA), was targeted in the process. This was the case, for example, when Ukraine's power grid was hacked in 2015. According to some experts, crippling a country's infrastructure through attacks against SCADA systems could evoke Article 5, and NATO's response could be more serious. [65]

In all, these events were a turning point for cybersecurity for Estonia, the EU, and NATO. They demonstrated the resilience of the country and the true asset that collaboration between nations could be for collective cybersecurity. But they also exposed some of these same actors' vulnerabilities and showed that they were on a learning curve. A nation like Russia, which might be willing to undermine another nation and stir inner tension, was now able to do this without ever setting a foot there in the first place.

According to Howard Schmidt, a former cybersecurity advisor for the White House, these DDoS attacks could have been countered more effectively with the installation of better firewalls. But no nation had the power

[64] https://www.youtube.com/watch?v=oGZkCdpPLBE&t=34s. 3'10: Suleyman Anil.

[65] Andrzej Kozlowski, "Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan," European Scientific Journal Vol. 3 (February 2014). Available at: https://eujournal.org/index.php/esj/article/view/2941

at the time to tell its internet service providers (private actors), telecommunication companies, and other online businesses to do so, which made the country a vulnerable target.[66] Following the attacks, Estonia implemented a national cybersecurity strategic plan in 2008. Tallinn also became the host of the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE). The publication of the Tallinn Manual in 2013, which studied how international law could be applied to cybersecurity, was a milestone for the Centre. Furthermore, these events made Estonia push for more cybersecurity within the EU and NATO. Recently, Estonian Minister of Entrepreneurship and Information Technology Andres Sutt proposed a NATO-like expenditure rule for cybersecurity.[67] This would involve countries spending 2% of their GDP expenditure on cybersecurity.

As can be seen from the establishment of the NATO CCDCOE, these events proved to be learning experiences for other governments and organisations like NATO. Among those lessons was the fact that hybrid threats were real and present and called for a broadening of tools, not limited to military responses, to counter them.

To conclude, with the case of Estonia, cyberattacks reached new heights, marking the appearance of a new type of warfare: cyberwarfare. While these attacks, in particular, fell under the threshold of NATO's Article 5, they revealed the seriousness of this threat and how important it was for governments and NATO to develop adequate tools to counter them. Attacks on critical infrastructure like SCADA could very well invoke the use of stronger tools under NATO's Article 5. Indeed, this would not be the end of cyberwarfare, but rather the beginning. Seven years after the cyberattacks on Estonia, Ukraine fell victim to hacks perpetrated by Russian groups with suspected ties to the Russian government. These types of attacks would repeat and multiply over the following years, to eventually cripple the country's economy and politics in 2017.

Ukraine: A Laboratory for Russian Stakeholders to Hone their Cyber Weaponry

March-May 2014: The Central Election Commission's (CEC) hack that almost disrupted Ukraine's presidential elections

Relations between Ukraine and the Kremlin began to deteriorate in 2014, leading to the annexation of Crimea and the fleeing of former President Yanukóvich to Russia. At the same time as Russian troops entered Crimea, Ukraine was fighting cyberattacks designed to create confusion and cloud judgement. Cyberattacks have become a daily occurrence for the country, and that does not seem to be changing anytime soon. Instead, they have become a way for Russia to exert its influence and geopolitical power. At the same time, Ukraine seems to have become a testbed for enemies to try out their crafted cyberweapons. Following the annexation of Crimea, Russia targeted Ukraine's communication networks as a first step. On 4 March 2014, troops were seen tampering with the telecom company

[66] Larry Greenemeier, "Estonian Attacks Raise Concern Over Cyber 'Nuclear Winter'," 24 May 2007. Available at: https://stratcomcoe.org/pdfjs/?file=/cuploads/pfiles/cyber_attacks_estonia.pdf?zoom=page-fit

[67] Oliver Noyan, (2021), "Estonia proposes NATO-like expenditure rule for cybersecurity". Euractiv. Available at: https://www.euractiv.com/section/cybersecurity/news/estonia-proposes-nato-like-expenditure-rule-for-cybersecurity/

Ukrtelecom's fibre-optic cables, causing a loss of service for many users. At the same time, the Ukrainian security chief Valentyn Nalivaichenko confirmed that "an attack [was] under way on mobile phones of members of the Ukrainian parliament for the second day in a row". Ukraine retaliated with Denial of Service attacks on many Russian websites from 7 to 14 March 2014. [68] However, Russia had the last word in this cyber conflict, as a pro-Russian hacker named CyberBerkut hacked into the Central Election Commission's (CEC) servers. The group then infected the electoral networks with malware, four days before the May 2014 presidential election results were announced. This malware was intended to portray extremist Dmytro Yarosh as the winner of this election, with 37% of the national vote. Fortunately, Ukrainian emergency response teams managed to remove the malware just forty minutes before the election results were released.

While these cyberattacks remain small disruptions that could be countered, they show just how seriously the country needs to take cyber threats in the future to prevent Russia from undermining their economy and their democratic system. And yet, at that time, few experts believed that this could ever turn into a cyberconflict of the magnitude of the cyberattacks in Estonia. For example, Paul Rosenzweig, founder of Red Branch Consulting and formerly part of US Homeland Security, stressed that these cyberattacks would be of little significance alone and would need military assistance to cause real damage. In his own words: "Let's not overemphasise the importance of cyber. Tanks beat cyber-bullets.". [69]

December 2015: Inside the power grid hack that plunged Ukraine into the dark

Source: SPxfuel, https://www.pxfuel.com/en/free-photo-irpjv

Security solutions

[68] Marie Baezner and Patrice Robin, (2018), "Hotspot Analysis: Cyber and Information Warfare in the Ukrainian Conflict" [online]. Available at: https://www.researchgate.net/publication/322364443_Cyber_and_Information_warfare_in_the_Ukrainian_conflict

[69] Dave Lee, (2014), "Russia and Ukraine in cyber 'stand-off'". BBC News. Available at: https://www.bbc.co.uk/news/technology-26447200

Those experts were proven wrong on 23 December 2015 as Ukraine saw its power grid hacked by the Russian government-affiliated group Sandworm, who cut the power for over 220,000 Ukrainian citizens. This was a direct attack on the country's critical infrastructure, which took a lot of preparation and ingenuity, that could have caused a lot more damage than it did.

But the attack started much earlier than December 2015. In the Spring of 2015, Sandworm undertook a large spear-phishing campaign to obtain credentials from IT staff and system administrators working for three firms that distributed electricity throughout Ukraine. In other words, Sandworm's hackers sent messages carefully crafted to each receiver's profile, hoping they would open those emails and the pseudo Word documents provided. If the recipients opened said Word documents, a pop-up notification would require them to enable macros, and, if they complied, the hackers would obtain the credentials for corporate networks. This campaign proved very effective as the hacktivists obtained the information they needed to eventually access the power grid's SCADA system. Sandworm also conducted reconnaissance work over several months to map out the existing SCADA networks and obtain access to the Windows Domain Controllers. This allowed them to control the breakers that managed how much power was produced and reconfigure the backup generators in case of emergency. It is believed that the hackers managed to go six months undetected as they obtained access and acquired privileges to the different systems of those power plants and were able to plant all the necessary Blackenergy3 malware for their future operation to be a success.[70] In this way, the Russian hackers could be sure that not only every single user of these companies would be plunged in the dark, but also that the operators who would deal with the issue would have to work in the dark.

This is how, on the night of 23 December 2015, around 225,000 citizens living in Western Ukraine were left without electricity to light their houses and offices or heat for their water and radiators. Sandworm's hackers started opening the breakers, and there was nothing the power plant's operators could do. To buy themselves even more time, Sandworm simultaneously launched a telephone Denial of Service attack against customer call centres preventing users from reporting the outage. This allowed them to take many substations offline before the operators even realised what was happening, taking down three power distribution centres and around 60 substations in the end.

Power was restored after six hours. Most users even got their electricity and heating back one to six hours after the attack. However, according to a US report, these power centres were still not fully operational even months after the attack.[71] Indeed, the Blackenergy3 that was installed destroyed much of the firmware and essential infrastructure within the power centres, leaving them unusable. Operators working onsite, for example, still had to control the breakers manually two months later, despite power being restored.

What is curious is that much more damage

[70] Pavel Politjuk et al, (2017), " Ukraine's power outage was a cyber attack: Ukrenergo". Reuters. Available at: https://www.reuters.com/article/us-ukraine-cyber-attack-energy-idUSKBN-1521BA

[71] Cybersecurity and Infrastructure Security Agency, "ICS Alert (IR-ALERT-H-16-056-01): Cyber-attack against Ukrainian critical infrastructure". Available at: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

could have been done. It is believed that Sandworm aimed for physical destruction and to cause far more lasting damage than a minor power outage for a few hours. Indeed, the installation of a malware named Industroyer aimed to disable protective relay failsafes (which would serve to restore power manually). This meant that as soon as operators tried to restore the power manually, they would create a massive power overload, frying lines and transformers. Had this worked, the attack would have made far more lasting damage, caused by operators simply trying to respond to the attack. However, a mistake was most probably made by the hackers, thus avoiding this worst-case scenario.

That mistake may not be made in the future. It is worrying to think that Russia had an appetite for destruction and was willing to jeopardise countless human lives. An attack during the peak of winter, aiming to deprive Ukrainians of power for what could have been weeks, would have, without doubt, made numerous casualties. Ukrainian cybersecurity experts would need to be on the lookout and simultaneously strengthen the country's cyber-resilience as more attacks were sure to come.

June 2017: The cyberattack that cost Ukraine $10 Billion and crippled its economy

And they didn't have to wait long. Less than two years later, Ukraine was hit by what the Trump administration qualified as the "most destructive and costly cyber-attack in history"[72]: NotPetya, also dubbed GoldenEye.

Ukraine's Constitution Day is celebrated on 28 June each year. It is meant to be a day of rest for the whole country, spend time with family and friends, and be free of any kind of worry. However, Russia and pro hackers had different plans for the country when they executed the NotPetya attack on 27 June 2017, at around 14:00 local time.

A malware disguised as ransomware infected computers asking victims to pay ransoms of $300 in Bitcoin to be able to use their computer again. The hackers amassed a total of $10,000 in this way before payments were cut off.[73] Ransomware is meant to infect systems and then requires a payment to unlock said systems. However, this was not ransomware: the aim of this attack was far from being purely financial. This malware exploited flaws in an update to an accounting software called MeDOC, compromising said update, and making it a key infection vector.

NotPetya was the largest cyberattack ever seen. It affected Ukrainian banks like Oschadbank, the country's power grid, the government's ministries, the media, transport infrastructure like Kiev's airport and metro lines, services like the post office, and even the Chernobyl power plant. While the 2007 cyberattacks on Estonia managed to disrupt the economic, social, and political spheres for over a week, this attack, which used malware instead of DDoS attacks, would cause lasting damage in Ukraine.

A major feature of this attack is that the malware seemed to spread through automation instead of human interference, allowing NotPetya to infect over 200,000 computers in the

[72] Trump White House, Statement from the Press Secretary (15 February 2018). Available at: https://trumpwhitehouse.archives.gov/briefings-statements/statement-press-secretary-25/

[73] Laurens Cerulus, (2019), "How Ukraine became a test bed for cyberweaponry". Politico Pro. Available at: https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/

space of a day. Moreover, this malware was highly sophisticated given that it managed to retrieve passwords, privileges, wipe files, and deal with data quite efficiently. According to a BBC Future interview with Oleh Derevianko, the head of Kiev-based cybersecurity firm Information Systems Security Partners (ISSP), the malware "was able to recognise specific 'hashes' on machines and networks and seemingly leave them alone. In short, it was more surgical than typical malware in what it attacked".[74]

While the attack only targeted Ukraine, it ended up affecting computers around the world. Companies like the American pharmaceutical company Merck, the British advertiser WPP, and the Danish shipping and energy company Maersk were all affected. The cyberattack ended up costing Maersk around $300 million in lost revenue.[75] In turn, WPP, the largest advertising company in the world, suffered a financial cost of $15 million. Given the substantial impact this attack had on companies that were not even targeted in the first place, it is not hard to believe that these cyberattacks crippled Ukraine, costing it billions in US dollars.

The reason for this is that it was not really a ransomware attack. The ransom which popped up on hacked computers was just a disguise. As many experts point out, the main purpose of the GoldenEye operation was not financial but to destroy as much as possible and create chaos within Ukraine. That is exactly what NotPetya did: it destroyed data and made it impossible to reboot computers. Even if victims paid the ransom, there was no way for them to recover the data lost. This explains how NotPetya cost Ukraine so much: businesses lost money paying fake ransoms and lost revenue through irrecoverable data and lost equipment due to the hacks. Additionally, foreign companies felt warier about conducting business in Ukraine after these events. Given the unprecedented impact this attack had on the world, experts have felt compelled to give this type of relentless attack a new name: Massive Coordinated Cyber Invasion. [76]

So, who was behind this Massive Coordinated Cyber Invasion? Experts were initially quite cautious in attributing it to anyone, given that so many countries saw themselves affected. However, with time, they were able to find similarities between the 2017 malware and past malware used by Russian hack-groups, including BlackEnergy3 (used in 2015) and KillDisk. Since then, the hackers who created NotPetya were certainly the same ones responsible for the 2015 Ukraine power grid attacks, namely Sandworm who are believed to have ties to the Russian government.

Therefore, the 2017 attacks that affected all of Ukraine's industries were part of Russia's strategy to destabilise the country and undermine its credibility as a state and place for business. Moreover, the attacks were a great way for Russian hacking groups to test out a new cyberweapon, use Ukraine once again as a testbed for said purpose, and keep building its cyber arsenal.

74. Christian Borys, (2017), "The day a mysterious cyber-attack crippled Ukraine". BBC. Available at: https://www.bbc.com/future/article/20170704-the-day-a-mysterious-cyber-attack-crippled-ukraine

75. Danny Palmer, (2017), "Petya ransomware: Cyberattack costs could hit $300m for shipping giant Maersk". ZD Net. Available at: https://www.zdnet.com/article/petya-ransomware-cyber-attack-costs-could-hit-300m-for-shipping-giant-maersk/

76. Supra note 75.

2017-Onwards: Why collaboration matters.

The 27 June 2017 will be remembered as a lost battle in this cyberwar with Russia. Since then, both NATO and the EU have intensified their interaction with Ukraine. Despite being neither a member of the EU nor NATO, it does enjoy privileged relationships with both organisations. For example, Ukraine is part of NATO's enhanced opportunity partner interoperability program. As we will see later in this study, this is a defining element of the Ukraine-NATO relationship.

Ukraine also enjoys bilateral assistance deals with the European Union, which extended to cyber assistance after the NotPetya attacks. As Lithuania's Vice Minister of National Defence Edvinas Kerza asserted when talking about Lithuania-Ukraine relations, "We provided them with political support, we've supported Ukraine in providing guns and ammo. Now we're moving to cyber". [77] So far, this partnership has had much success, and Ukraine's 2019 presidential elections ran smoothly.

The situation in Ukraine is very relevant for the European Union. As we have been evaluating, the European Union's cybersecurity is and should be a priority. Indeed, what has been happening over the last decade in Ukraine could easily happen in any EU's countries. Therefore, bodies like the Joint Cyber Unit and ENISA, directives like NIS 2, and the EU's cyber strategy overall matter so much. Likewise, the EU's relationship with NATO is crucial, and the two must keep up with cyber threats that are becoming ever-more dangerous over time.

EU-NATO COOPERATION ON CYBERSECURITY

Common Developments

As discussed earlier in this paper, cybersecurity policies have long been established in the EU and NATO. However, the issue of cybersecurity has only recently become a constituent component of their agendas, triggered by the 2007 cyberattacks in Estonia. In this regard, NATO created its Cyber Defence Policy in 2008. Following this, the EU established its first common Cyber Security Strategy in 2013.[78]

The large-scale incident in Estonia, together with the 2014 attacks on the Ukrainian cyberspace, prompted the EU and NATO to enhance their cooperation and implement common strategies to reinforce cybersecurity. As a result, on 8 July 2016, the President of the European Council, the President of the European Commission, and the Secretary-General of NATO signed a Joint Declaration, which would create a concrete legal framework for common assurance of cybersecurity and de-

[77] Supra note 74.
[78] Supra chapter 1.2.

fence.[79]

The Declaration's legal implementation plan includes four areas of cooperation: the integration of cyber defence into operations and missions; education and training; exercises; and standards.

It is important to note that, through the legal implementation of the abovementioned Declaration, enhanced coordination in maritime issues was established, characterised by logistical support and information sharing between the two operations of EU Naval Force Sophia in the Mediterranean and Sea Guardian. Furthermore, the two organisations implemented a closer defence and security cooperation in the field of Military Aviation, which was later accompanied by the introduction of the Military Airworthiness arrangements and Aviation security strategies, including those for cyberspace. The EU and NATO also exchanged views on integrating several aspects of cybersecurity into the planning and conducting of relevant operations and missions to further develop their interoperability in cyber defence standards and requirements. Furthermore, to strengthen and further develop their cooperation in training, the EU and NATO harmonised the necessary training requirements and established training courses characterised by mutual participation. Regarding the fourth area of cooperation, the organisations implemented coordinated exercises as a pilot project based on reciprocity.[80] That same year, the Cyber Defence Pledge was established to further develop cyber resilience. Its main aim was to strengthen the cyber defences of the national networks and infrastructures of the Member States.[81]

Cybersecurity was recognised as one of the main priorities of the Global Strategy for the European Union's Foreign and Security Policy. Thus, in 2017, the EU carried out a legal revision of the first EU Cyber Security Strategy, which was later included in the Cybersecurity Package, adopted that same year. The main purpose of the revision was to update the first EU Cyber Security Strategy, improve the EU's critical infrastructure, and boost the EU's digital self-assertiveness. In the legal revision, the EU did not make sufficiently clear how to overcome the lack of legal authority in cybersecurity issues. Still, it emphasised that the Member States should enhance the legal regulation of cybersecurity at the national level and the supranational level.[82]

In the clime of the international cyber threats, the EU and NATO perceive themselves as crucial complementary partners with a common aim to establish cyber defence mechanisms and to strengthen their overall cyber resilience. Therefore, on 10 February 2016, the organisations signed the Technical Arrangement on Cyber Defence. The function of the Arrangement revolves around the exchange of relevant cybersecurity data to allow the organisations not only to predict and detect potential cyber-attacks, but also to undertake appropriate counteractive measures. According to the NATO Communications and Information Agency General Manager, "information exchange is crucial to cyber defence". The signing of the Technical Arrangement

[79] Joint Declaration by the president of the European Council, the president of the European Commission and the secretary general of NATO (8 July 2016), (online). Available at: https://www.consilium.europa.eu/media/21481/nato-eu-declaration-8-july-en-final.pdf

[80] Ibid.

[81] North Atlantic Treaty Organization, "Cyber Defense," Updated November 10, 2017

[82] Joint Communication to the European Parliament and the Council," JOIN, 2017: 0450 final (online). Available at: https://eurlex.europa.eu/legalcontent/en/TXT/?uri=CELEX%3A-52017JC0450

serves as a pivotal milestone in strengthening the cooperation between the EU and NATO in the sphere of cyber resilience.[83]

Despite the undeniable development in the direction of a common cyber defence strategy, the relationship between the EU and NATO remains complicated. There are currently three main obstacles that prevent the effective implementation of this cooperation.

The first obstacle consists of a lack of information sharing and a lack of international awareness. Even though the Technical Arrangement was adopted in 2016, the Member States of both organisations cannot successfully share relevant information to respond to cyberattacks, leading to a lack of shared international awareness between States regarding cyber threats.[84] This results in the incompleteness of the current declarations of the EU and NATO regarding their capabilities. Furthermore, in most instances, NATO does not share classified information with the EU. Lastly, some of the Member States that have more developed technologies to detect cyber threats refuse to share the classified information with others, resulting in a more complicated attribution and response to potential cyber incidents.

The second obstacle is the lack of equality in regard to the level of preparedness and cyber resilience on a national level of the two organisations' Member States. Even though the EU and NATO aim to coordinate the national efforts in cyberspace, this goal remains complicated since their recommendations to Member States are not legally binding. Moreover, the Member States remain sceptical in regard to potential external assistance by supranational bodies such as the EU or NATO even when they need to develop their national cyber resilience. This lack of trust stems precisely from the information sharing issues described above.

The third obstacle is the limitation of joint cyber education, training, and exercises between the EU and NATO. The two organisations only held one joint military exercise in 2003, and even today, despite the theoretical development of their cooperation in the cybersphere, their efforts towards achieving cyber resilience are practically separate.[85] Therefore, the primary objectives to be achieved jointly by the EU and NATO are the successful cooperation in cybersecurity and the implementation of necessary legislation and legal measures to detect and prevent cybersecurity threats and hold perpetrators accountable.

The abovementioned cooperation can be achieved first by establishing a Joint Cyber Threat Analysis Hub whose role is to analyse and share strategic level reports in regard to response mechanisms in times of crisis activated by the EU and NATO in specific situations. Second, it can be achieved by establishing a Joint Committee for cyber research and cyber innovation to reduce inequality regarding preparedness among Member States and address the technology gaps between the private and public sectors in these states. Third, it can be achieved by establishing a peer-assessment process to identify the resilience and capabilities gaps between Member States.[86]

[83] The EU-NATO Technical Arrangement on Cybersecurity (10 February 2016), (online). Available at: https://www.nato.int/cps/en/natohq/news_127836.htm
[84] Bruno Lete & Piret Pernik, "EU-NATO Cybersecurity and Defense Cooperation: from Common Threats to Common Solutions", (15 December 2017), pg. 2-4
[85] Ibid
[86] Ibid, pg. 3-5

EU-NATO Cooperation in Ukrainian Cyberspace

Thus far, we have analysed the theoretical cooperation between the EU and NATO in the field of cybersecurity. This cooperation is characterised by common developments aiming to achieve a similar objective: ensuring a sufficient level of cyber resilience throughout the Member States of the two organisations. The following section will present the practical application of this cooperation, more specifically concerning the case of Ukraine and the recent cyber-attacks towards it.

Although Ukraine has a lot of experts in the cybersphere and thus the potential to tackle cyber crime on a domestic level, it is characterised by a lack of international backing. Therefore, Ukraine's cooperation in cybersecurity with the EU and with NATO is exercised separately, with both organisations coordinating their efforts, mainly at the level of practical assistance toward Ukraine, in accordance with the principles of their cooperation in cybersecurity. In terms of the relationship between the EU and Ukraine, cybersecurity plays a crucial role. This is why the EU pays special attention to how the country implements its cybersecurity policies. The EU itself, in the cooperation with Ukraine, is guided by the objectives set out in the Joint Staff Working Document on "Eastern Partnership – 20 deliverables for 2020: focusing on key priorities and tangible results".

Source: Flickr, https://www.flickr.com/photos/descrier/35440117101

EU data protection and digital security
Babak Fakhamzadeh

The three main objectives set out in the above-mentioned legal document consist in creating specific operating units to fight cybercrime, developing public and private cooperation, and developing international cybersecurity cooperation. Eventually, by the end of 2020, Ukraine fulfilled these obligations.

In addition, Ukraine has implemented the Criminal Cybercrime Convention[87] and Directive 2008/114/EC[88] on protecting critical infrastructure. On 17 December 2018, during the fifth meeting of the Association Council in Brussels, both Ukraine and the EU expressed the need for further cooperation in regard to the cybersphere.[89]

The EU, under the Technical Assistance and Information Exchange legal instrument, implemented the creation of a specific legislative framework regarding cybersecurity in Ukraine and promoted further development of the national cybersecurity structures. Furthermore, the EU assisted Ukraine in its national fight against cyber threats through its Advisory Mission to Ukraine (EUAM). The mission itself promoted the enforcement of Ukrainian law regarding cybersecurity.[90]

Indeed, the cybersecurity cooperation between the EU and Ukraine is crucial for both sides, but it is also a priority element in the cooperation between Ukraine and NATO.

On 9 February 2017, during a discussion between representatives of the two parties on Non-Military Cooperation as Response to Common Hybrid Threats, cybersecurity was set in second place among the priorities of the joint Ukraine-NATO cooperation.[91] This co-operation is also registered every year in the Annual National Program under the guidance of the Ukraine-NATO Commission. The main aim of such common actions is to improve the Ukrainian national legislative framework on cybersecurity and ensure national technical mechanisms to fight cyber threats in general, specifically the cybersecurity threats coming from Russia. Furthermore, it aims to bring the Ukrainian IT sector to the same level as the one used by the EU and NATO against cyber threats and to further develop the Ukrainian cyber defence. These developments are financed by the Trust Fund, launched for the first time in 2014, to establish Ukraine's own anti-cyber threats groups and Computer Security Incident Response team capacity.[92]

Eventually, in 2017, Ukraine received the appropriate technical mechanisms and equipment to fight cybercrime, and the first stage of the Trust Fund was completed.

Many representatives of the Ukrainian government also receive technical equipment from NATO to protect the information structure. Moreover, in 2018 a Situational Centre was established, to provide cybersecurity for the State's service systems. It is also relevant to mention that NATO has allocated approximately 1 million dollars for this project, demonstrating its determination towards achieving effective cyber cooperation. In addition, Ukraine participates in relevant NATO cybersecurity training programs and

[87] Convention on Cybercrime (23 November 2001), (online). Available at: https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf

[88] Directive 2008/114/EC, (8 December 2008), (online). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2008.345.01.0075.01.ENG

[89] Joint press release following the 5th meeting of the Association Council between Ukraine and the EU (17 December 2018)

[90] Marikki Rieppola, "The EU Advisory Mission in Ukraine: Normative or Strategic Objectives?", (February 2017), pg. 6-7

[91] Ukraine-NATO: Non-Military Cooperation in Joint Response to Hybrid Threats (9 February 2017)

[92] NATO's practical support to Ukraine (December 2015), (online). Available at: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2015_12/20151130_1512-factsheet-nato-ukraine-supportr_en.pdf

its Multinational Training called the Coalition Warrior Interoperability Exercise.[93]

To conclude, Ukraine eventually cooperates successfully with both the EU and NATO in the cybersecurity sphere. Still, it is important to note that this cooperation is carried out with each organisation separately. This means that despite further development of the EU-NATO cooperation in cybersecurity and the implementation of relevant joint legal documentation, there is still room for improvement, particularly concerning the interaction with third countries, such as Ukraine.[94]

CONCLUSION

In all, the European Union, its Member States, NATO, and stakeholders like Ukraine have come a long way in protecting their cyberspaces. Less than two decades ago, the European community's cybersecurity relations were governed by informality and a *quid pro quo* principle regarding the circulation of relevant information between Member States. Similarly, cybersecurity didn't yet form part of the EU-NATO agenda. Less than a decade ago, Ukraine went through the worst cyberwar to date, completely underprepared, overwhelmed, and with virtually no allies.

Fifteen years later, we can see multiple developments on all fronts. Measures taken like NIS 2 Directive, the formation of ENISA, and the proposal to create a Joint Cyber Unit, show an ever-increasing amount of mutual awareness towards cyber threats.

Likewise, the Estonian cyber crisis highlighted the need for NATO to pull its forces together to fight cyber threats collectively. This has since been advanced through various actions such as the Cyber Defence Pledge in 2008, and the 2016 Technical Arrangement on Cyber Defence which strengthens EU-NATO cooperation.

Lastly, both organisations have also recognised the importance of working jointly with third parties. The Ukrainian cyberwar highlights the need for the EU and NATO to treat said external cyberspace as if it were its own. As we were able to see throughout this paper, many steps have been taken towards this.

Despite progress, however, we've also observed many persisting flaws in cyber relations. Said flaws mainly concern relations between the EU and NATO and between Member States within the European Union.

Within the Union, despite efforts to increase cyber awareness, relations between Member States are still characterised by a reticence to share information and cyber data. As a result, there is still a lack of collective situational awareness about cyberthreats. Additionally, no mechanism to counter large-scale, cross-border cyber incidents or crises exists. That's why both ENISA's and the JCU's role should be particularly interesting in the times to come. Both bodies should provide Member

[93] Enhancing Cybersecurity in Ukraine (29 October 2018), (online). Available at: https://www.nato.int/cps/en/natohq/news_159840.htm
[94] Ibid

States with collective cyber-education, assist with third parties, and facilitate sharing cyber data within the European community.

As for the relationship held between the EU and NATO, reticence and scepticism regarding the alliance seem to be the main problem. So far, the alliance's potential in the cyber area is being undermined by a lack of information sharing, a lack of shared international awareness, and an unequal preparation among allies to counter cyber threats. As we have seen, the solution lies in deepening ties and promoting joint strategic research that might prove useful to the alliance's reliability.

All relevant actors can only benefit from taking these steps. The priority lies in increasing collective cybersecurity and deepening the collaboration between States and international organisations. Past crises like the ones presented in this paper have shown how crucial it is to work together to provide a comprehensive approach to fighting digital threats. Indeed, what has been happening in Ukraine is only right beside us, and it is not far-fetched to think it could happen anytime within our borders. Collective action is the solution to this problem.

BIBLIOGRAPHY

Askoxylakis Ioannis. (2019). 'Blueprint – European coordinated response to large-scale cybersecurity incidents and crises', European Commission [online]. Available at: https://www.enisa.europa.eu/events/artificial-intelligence-an-opportunity-for-the-eu-cyber-crisis-management/workshop-presentations/20190603-ec-blueprint.pdf [Accessed: 14 September 2021].

Autolitano, Simona. (2020), 'A Europe Fit for the Digital Age: The Quest for Cybersecurity Unpacked', Istituto Affari Internazionali. [online] Available at: https://www.iai.it/en/pubblicazioni/europe-fit-digital-age-quest-cybersecurity-unpacked [Accessed: 14 September 2021].

Azeez, Nureni Ayofe and Barry Irwin. (2010). "Cyber Security: Challenges and the Way Forward", Computer Science & Telecommunications 29, no. 6 (2010): 56-69. [online] Available at: https://www.researchgate.net/publication/265121167_CYBER_SECURITY_CHALLENGES_AND_THE_WAY_FORWARD [Accessed: 12 September 2021].

Baezner, Marie and Robin, Patrice. (2018), "Hotspot Analysis: Cyber and Information Warfare in the Ukrainian Conflict" [online]. Available at: https://www.researchgate.net/publication/322364443_Cyber_and_Information_warfare_in_the_Ukrainian_conflict [Accessed: 14 September 2021].

Borys, Christian. “The day a mysterious cyber-attack crippled Ukraine”. BBC. Available at: https://www.bbc.com/future/article/20170704-the-day-a-mysterious-cyber-attack-crippled-ukraine [Accessed: 14 September 2021].

Burstein, Aaron J. (2008). “Toward a Culture of Cybersecurity Research”. [online] Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1113014 [Accessed: 12 September 2021].

CERT-EU, (2021). ‘About Us’. [online] Available at: https://www.cert.europa.eu/cert/plainedition/en/cert_about.html [Accessed: 14 September 2021].

Cerulus, Laurens. “How Ukraine became a test bed for cyberweaponry”. Politico Pro. Available at: https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/ [Accessed: 14 September 2021].

Clark, Kas, Don Stikvoort, Eelco Stofbergen and Elly van den Heuvel. “A Dutch Approach to Cybersecurity Through Participation.” IEEE Security & Privacy 12, no. 5 (September 2014): 27-34.

Convention on Cybercrime (23 November 2001), (online). Available at: https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf [Accessed: 29 September 2021].

Cybersecurity and Infrastructure Security Agency, “ICS Alert (IR-ALERT-H-16-056-01): Cyber-attack against Ukrainian critical infrastructure”. Available at: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01 [Accessed: 14 September 2021].

Directive 2008/114/EC, (8 December 2008), (online). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2008.345.01.0075.01.ENG [Accessed: 29 September 2021].

Enhancing Cybersecurity in Ukraine (29 October 2018), (online). Available at: https://www.nato.int/cps/en/natohq/news_159840.htm [Accessed: 29 September 2021].

European Commission, (2013). ‘EU Cybersecurity plan to protect open internet and online freedom and opportunity’. [online] Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_13_94 [Accessed: 12 September 2021].

European Commission, (2013). ‘European Cybercrime Centre (EC3) opens on 11 January’. [online] Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_13_13 [Accessed: 12 September 2021].

European Commission. ‘Joint Communication to the European Parliament and the Council – The EU’s Cybersecurity Strategy for the Digital Decade’, JOIN/2020/18.

European Commission, (2020). ‘New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient’. Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391 [Accessed: 12 September 2021].

European Commission, (2020). ‘NIS Directive’. [online] Available at: https://digital-strategy.ec.europa.eu/en/policies/nis-directive [Accessed: 11 September 2021].

European Commission. “Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive 2016/1148”, COM/2020/823.

European Commission, (2021). ‘2021 State of the Union Address by President von der Leyen’. [online] Available at: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_21_4701 [Accessed: 25 September 2021].

European Commission, (2021). ‘Establishment of a local office presence of ENISA in Brussels, Belgium’. [online] Available at: https://digital-strategy.ec.europa.eu/en/news/establishment-local-office-presence-enisa-brussels-belgium [Accessed: 14 September 2021].

European Commission, (2021). ‘The Cybersecurity Strategy’. [online]. Available at: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy [Accessed: 12 September 2021].

European Commission, (2021). 'The EU Cybersecurity Act'. [online] Available at: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act [Accessed: 12 September 2021].

European Commission, (2021). 'The Joint Cyber Unit'. [online] Available at: https://digital-strategy.ec.europa.eu/en/policies/joint-cyber-unit [Accessed: 14 September 2021].

European Parliament and Council of the European Union. "Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency", OJEU L077/2004.

European Parliament and Council of the European Union, "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union", OJEU L194/2016.

European Parliament and Council of the European Union, "Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)", OJEU L151/15.

Géant, (2021). 'TF-CSIRT: Computer Security Incident Response Teams'. [online] Available at: https://www.geant.org/People/Community_Programme/Task_Forces/Pages/TF-CSIRT.aspx [Accessed: 10 September 2021].

Greenemeier, Larry. "Estonian Attacks Raise Concern Over Cyber 'Nuclear Winter'," 24 May 2007. Available at: https://stratcomcoe.org/pdfjs/?file=/cuploads/pfiles/cyber_attacks_estonia.pdf?zoom=page-fit [Accessed: 14 September 2021].

Ivanov, Sergei. Quoted in: "Here We Go Again," The Baltic Times, 4 April 2007. Available at: https://www.baltictimes.com/news/articles/17635/ [Accessed: 14 September 2021].

Joint Communication to the European Parliament and the Council," JOIN, 2017: 0450 final (online). Available at: https://eurlex.europa.eu/legalcontent/en/TXT/?uri=CELEX%3A52017JC0450 [Accessed: 29 September 2021].

Joint Declaration by the president of the European Council, the president of the European Commission and the secretary general of NATO (8 July 2016), (online). Available at: https://www.consilium.europa.eu/media/21481/nato-eu-declaration-8-july-en-final.pdf [Accessed: 29 September 2021].

Kovács, László. "Cyber Security Policy and Strategy in the European Union and NATO." Land Forces Academy Review 23, no. 1 (2018): 16-24.

Kozlowski, Andrzej. "Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan," European Scientific Journal Vol. 3 (February 2014). Available at: https://eujournal.org/index.php/esj/article/view/2941 [Accessed: 14 September 2021].

Lee, Dave. "Russia and Ukraine in cyber 'stand-off'". BBC News. Available at: https://www.bbc.co.uk/news/technology-26447200 [Accessed: 14 September 2021].

Lete, Bruno and Pernik, Piret. "EU-NATO Cybersecurity and Defense Cooperation: from Common Threats to Common Solutions", (15 December 2017), pg. 2-4.

Lin, Herbert, Alfred Z. Spector, Peter G. Neumann, and Seymour Goodman, "Toward a Safer and More Secure Cyberspace". [online] Available at: https://www.researchgate.net/publication/220426062_Toward_a_safer_and_more_secure_cyberspace [Accessed: 12 September 2021].

NATO's practical support to Ukraine (December 2015), (online). Available at: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2015_12/20151130_1512-factsheet-nato-ukraine-supportr_en.pdf [Accessed: 29 September 2021].

North Atlantic Treaty Organization, "Cyber Defense," Updated November 10, 2017.

Noyan, Oliver. "Estonia proposes NATO-like expenditure rule for cybersecurity". Euractiv. Available at: https://www.euractiv.com/section/cybersecurity/news/estonia-proposes-nato-like-expenditure-rule-for-cybersecurity/ [Accessed: 14 September 2021].

Palmer, Danny. “Petya ransomware: Cyberattack costs could hit $300m for shipping giant Maersk”. ZD Net. Available at: https://www.zdnet.com/article/petya-ransomware-cyber-attack-costs-could-hit-300m-for-shipping-giant-maersk/ [Accessed: 14 September 2021].

Putin, Vladimir (translated). ”Speech at the Military Parade Celebrating the 62nd Anniversary of Victory in the Great Patriotic War,” Kremlin.ru, 9 May 2007. Available at: http://en.kremlin.ru/events/president/transcripts/24238 [Accessed: 14 September 2021].

Politjuk, Pavel et al. “ Ukraine's power outage was a cyber attack: Ukrenergo”. Reuters. Available at: https://www.reuters.com/article/us-ukraine-cyber-attack-energy-idUSKBN1521BA [Accessed: 14 September 2021].

Rieppola, Marikki. “The EU Advisory Mission in Ukraine: Normative or Strategic Objectives?”, (February 2017), pg. 6-7.

Ruohonen, Jukka, Sami Hyrynsalmi, and Ville Leppänen. “An Outlook on the Institutional Evolution of the European Union Cyber Security Apparatus.” Government Information Quarterly 33, no. 4 (October 2016): 746-756.

The EU-NATO Technical Arrangement on Cybersecurity (10 February 2016), (online). Available at: https://www.nato.int/cps/en/natohq/news_127836.htm [Accessed: 29 September 2021].

“Transcript of Remarks and Replies to Media Questions by Russian Minister of Foreign Affairs Sergey Lavrov Following Ministerial Meeting of Russia-NATO Council, Oslo, April 27, 2007,” The Ministry of Foreign Affairs of the Russian Federation. Available at: http://www.mid.ru/en/press_service/minister_speeches/-/asset_publisher/7OvQR5KJWVmR/content/id/375128 [Accessed: 14 September 2021].

Trump White House. Statement from the Press Secretary (15 February 2018). Available at: https://trumpwhitehouse.archives.gov/briefings-statements/statement-press-secretary-25/ [Accessed: 14 September 2021].

Ukraine-NATO: Non-Military Cooperation in Joint Response to Hybrid Threats (9 February 2017).

Created in 1953, the Finabel committee is the oldest military organisation for cooperation between European Armies: it was conceived as a forum for reflections, exchange studies, and proposals on common interest topics for the future of its members. Finabel, the only organisation at this level, strives at:

- Promoting interoperability and cooperation of armies, while seeking to bring together concepts, doctrines and procedures;
- Contributing to a common European understanding of land defence issues. Finabel focuses on doctrines, trainings, and the joint environment.

Finabel aims to be a multinational-, independent-, and apolitical actor for the European Armies of the EU Member States. The Finabel informal forum is based on consensus and equality of member states. Finabel favours fruitful contact among member states' officers and Chiefs of Staff in a spirit of open and mutual understanding via annual meetings.

Finabel contributes to reinforce interoperability among its member states in the framework of the North Atlantic Treaty Organisation (NATO), the EU, and *ad hoc* coalition; Finabel neither competes nor duplicates NATO or EU military structures but contributes to these organisations in its unique way. Initially focused on cooperation in armament's programmes, Finabel quickly shifted to the harmonisation of land doctrines. Consequently, before hoping to reach a shared capability approach and common equipment, a shared vision of force-engagement on the terrain should be obtained.

In the current setting, Finabel allows its member states to form Expert Task Groups for situations that require short-term solutions. In addition, Finabel is also a think tank that elaborates on current events concerning the operations of the land forces and provides comments by creating "Food for Thought papers" to address the topics. Finabel studies and Food for Thoughts are recommendations freely applied by its member, whose aim is to facilitate interoperability and improve the daily tasks of preparation, training, exercises, and engagement.

FINABEL

Quartier Reine Elisabeth
Rue d'Evere 1 box 44
B-1140 BRUSSELS

Tel: +32 (0)2 441 79 05 – GSM: +32 (0)483 712 193
E-mail: info@finabel.org

You will find our studies at **www.finabel.org**

European Army Interoperability Centre

www.linkedin.com/in/finabelEAIC @FinabelEAIC @FinabelEAIC

Responsible publisher: Mario BLOKKEN - Finabel Permanent Secretariat - QRE - Rue d'Evere,1 - B-1140 Brussels - +32 (0)2 441 79 05