HADMÉRNÖK
VÉDELEMINFORMATIKA

19. évfolyam (2024) 1. szám 121–141.
DOI: 10.32567/hm.2024.1.7

Károly Kassai[1]

Emerging Challenges and New Responses, Building Capabilities to Counter Threats in Cyberspace

Questions and Answers on How to Improve Cybersecurity

Abstract

Cyberspace phenomena are changing rapidly at international and national levels. Growing threats, new vulnerabilities and protection against them require continuous action at the level of the EU, NATO and national competent authorities and organisations. Adequate protection of critical infrastructure and cyberspace is a vital strategic, operational and technical challenge for the EU, NATO and therefore nations. Cross-border impacts, threat actors and malicious actions require coordination of international and national procedures, mechanisms and cooperation. This article presents the most important phenomena and trends experienced today, as well as EU and NATO initiatives and requirements at the strategic level, illustrating what changes can be expected in cybersecurity.

Keywords: cybersecurity, critical infrastructure protection, cyber threat, vulnerability, security requirement

Introduction

The events, experiences, threats and new security requirements (and initiatives, regulations, recommendations) related to cyberspace constitute a constantly changing environment for states, governmental organisations, social and economic actors and citizens with varying impacts.

[1] E-mail: karoly.kassai@yahoo.com

Responsible organisations and actors are under pressure to continuously monitor threats and vulnerabilities in cyberspace, to identify impacts and malicious actors and to comply with international and national requirements.

Following international frameworks, trends and typical processes will support the development of national and military capabilities and the foundation of concepts and initiatives for more robust national cybersecurity and effective cyber operations.

The NATO and the EU has similar requirements and several common actions in the field of cybersecurity, as Kovács concludes,[2] and in line with this observation, it would be useful to examine the horizontally enhanced regulations and initiatives at a strategic level.

This study[3] aims to identify recent strategic changes in the international environment in the field of cybersecurity that may have implications on the national regulations to support the needed developments by competent authorities and organisations.

The study was carried out by analysing "first line requirements", initiatives, and related opinions as well as a high-level comparison of EU and NATO declarations and international/national-level opinions on cybersecurity.

Threats and responses at the strategic level

The NATO Strategic Concept (Concept) (2022) is a long-term strategic document for the Alliance, setting out its core missions and main lines of ambition in response to the current security environment and emerging threats. The main objective is the collective defence of the Allies "based on a 360-degree approach". NATO's core tasks are *deterrence and defence,*[4] *crisis prevention and management,* and *collective security.*

According to Szenes,[5] the change in core tasks from "defence and deterrence" to "deterrence and defence" is a clear response to the new security challenges.

The deterrence and defence functions are based on coordinated nuclear, conventional and missile defence capabilities, "complemented by space and cyber capabilities". The use of correct terminology should be a priority for the better understanding of the subject. It is not enough to categorise a force and identify it as a deterrent component. This answers the question of whether cyber operational capability alone is a deterrent or should be classified as a supporting force – today!

The Concept states that the security environment is becoming increasingly complex and unpredictable, which is clearly justifiable in cyberspace. One of the main challenges is the increasing frequency and sophistication of cyberattacks, which can have a significant impact on national security – and on other aspects as well (e.g. alliance, regional, international). The secure use of and free access to space

[2] Kovács 2018: 23.

[3] This article is an edited, extended version of a conference presentation held on 15 November 2023 (Budapest, Infocommunication 2023 Conference, "Strategic level changes in the cyberspace framework, major impacts/A kibertér keretrendszerének stratégiai szintű változásai, fontosabb hatások").

[4] This is an important change in focus because in the previous Concept, the formulation of tasks was "defence and deterrence".

[5] Szenes 2022: 7.

and cyberspace is a key factor in deterrence and defence. The Alliance will develop capabilities *using all possible tools to operate effectively in space and cyberspace*, addressing the full spectrum of threats.[6]

The EU Cybersecurity Strategy (2020) – as a strategic baseline – outlines a comprehensive approach to cybersecurity for the long term (ten years) to counter cyber threats. The strategy sets out three main pillars to strengthen cybersecurity across the EU:

- *Enhancing resilience.* Critical areas for development are resilient infrastructure and critical services, European Cyber Shield, secure communication infrastructure (e.g. satellite, quantum communication infrastructure), next generation networks, secure IoT,[7] supply chain security.[8]
- *Strengthening cyber operational capabilities for prevention, deterrence and response.* Key capability areas are the EU Joint Cyber Unit initiative, coordinated response to large-scale cybersecurity incidents and crises ('Blueprint'), cyber diplomacy toolbox, development of cyber defence capabilities (modernisation of the Cyber Defence Policy Framework, Military Vision and Strategy on Cyberspace as a Domain of Operations, Military CERT[9] Network and various EDA[10] cyber-related projects).[11]
- *Promoting a global and open cyberspace.* Key activities are international standardisation processes, efforts towards "responsible state behaviour in cyberspace", international cooperation (e.g. EU Cyber Diplomacy Network, EU–NATO cooperation), strengthening of the Budapest Convention on Cybercrime.[12]

Bihaly notes[13] that the key areas of the strategy are at different stages of development. The actors of the various processes (nations, EU institutions, organisations and agencies) still have a lot of work ahead to achieve coherence between organisations.

The next EU regulations and initiatives, which will be presented later, will demonstrate the different steps alongside the direction of the Cybersecurity Strategy.

The EU Strategic Compass for Security and Defence (Compass) (2022) document provides guidance and aims to strengthen security and defence policy in the EU with four pillars: *act, invest, partner* and *secure* by 2030.

The Compass highlights *strategic competition* and *complex security threats* in the security landscape. The frequency and impact of hybrid threats are increasing, and interdependencies (e.g. digitalisation) may cause more problems than before. Global commons (e. g. seas, space and cyberspace) are contested domains. The EU has an interest in *exploiting all operational domains* (land, sea, air, cyber and space). The EU will strengthen the elements of Cyber Defence Policy, improve cyber

[6] NATO 2022b: 6, 7.
[7] IoT: Internet of Things.
[8] European Commission 2020: 5–12.
[9] CERT: Computer Emergency Response Team.
[10] EDA: European Defence Agency.
[11] European Commission 2020: 13–18.
[12] European Commission 2020: 19–22.
[13] Bihaly 2021: 54.

intelligence capabilities for effective cyber resilience,[14] and enhance interoperability and information sharing capabilities among cyber organisations for more effective cooperation (e.g. cyber exercises).

The Compass notes that the new EU Space Strategy for Security and Defence will play an important role[15] in better understanding space-related risks and threats.

The Compass identified the need to strengthen command and control structures (e.g. military planning and conduct capability, strategic communication tools) to support EU-led missions and operations.[16]

Regarding conflicts and crises, Novák-Varró underlines[17] the spread of the concept of "integrated approach" in the EU's strategic thinking. Another important element is that the content of the former "national defence-oriented" resilience has changed and now includes the complex aspects of human security.

In line with the findings of the Compass, Kersánszky confirms[18] that cyberspace has become an area of geopolitical competition, requiring decisive and rapid responses to malicious cyber activities. The EU must place great emphasis on prevention, protection, early detection and countermeasures at military, civilian and political levels.

At the 2021 NATO Summit, the Alliance adopted the *Comprehensive Cyber Defence Policy,*[19] which *reinforces NATO's defence mandate* and commitment to actively deter, defend and counter cyber threats in support of NATO's three core tasks and its overall deterrence and defence posture.

Responses will be collective, using *political, diplomatic* and *military* tools. Significant malicious cyber activity may be considered an armed attack. NATO's comprehensive approach to cyberspace focuses on unity of effort at the political, military and technical levels.

The Alliance remains committed to compliance with international law, promoting a free, open and secure cyberspace, and supporting responsible state behaviour in cyberspace.[20]

The Hungarian approach is similar to the NATO and EU documents, mentioned in the Hungarian National Security Strategy (2020) (e.g. comprehensive approach to security, hybrid threat orientation, intelligence-led decisions). Szenes confirms[21] that the strategy addresses the hybrid threat with a two-level solution (national and alliance) supported by whole-of-government resources.

According to Kovács's interpretation,[22] the importance of information and communication systems, which ensure the functioning of society, has increased in

[14] The networks, digital services (including military, critical infrastructure and governmental services) will be more robust and secure by the requirements of the new Cyber Resilience Act (2022).

[15] Accessibility and operational capabilities of space objects have critical importance in the field of digital infrastructure and communications.

[16] European Union External Action 2022: 2, 3, 5, 14, 23.

[17] Novák-Varró 2021: 36–37.

[18] Kersánszky 2022: 74.

[19] This Policy is the NATO's highest-level strategic document on cyber defence in the support of NATO's Strategic Concept (similar in function to the EU's Cyber Security Strategy). The content is based on NATO's public extract.

[20] NATO 2021a.

[21] Szenes 2021: 45.

[22] Kovács 2020: 17.

the strategy. The protection of these systems is a national security interest (and a strategic object).

Bányász et al. conclude[23] that according to the strategy, national cyber defence cannot function without international cooperation. This cooperation is primarily within the Alliance system, which is based on trust to act quickly and effectively.

The new risks and threats in the security environment will have an impact on the Strategy, so its next revision *should consider the effects of the latest factors, threats and new technologies.* After main changes, the lower-level strategies and regulations should be updated (e.g. National Cyber Security, National Military Strategy and their supporting documents).

High-level risk identification

The EU Economic Security Strategy (2023) identifies the key considerations for the main risk types as follows:

- resilience of supply chains, including energy security
- physical and cybersecurity of critical infrastructure
- technology security and technology leakage and
- weaponisation of economic dependencies or economic coercion[24]

Based on strategic level considerations, the *EU Commission Recommendation on critical technology areas has prioritised and identified the highest level risks* (2023), which are *advanced semiconductor technologies, artificial intelligence technologies, quantum-* and *biotechnologies,* and they require urgent risk mitigation actions.[25]

The EU Space Strategy[26] (2023) underlines the *importance of the space segment,*[27] including *space objects, communication tools* and the fundamental importance of *open access* for the EU. The strategy states that critical infrastructure and communication requirements must apply to both space objects and ground facilities to ensure a safe and secure space. Member States should take *measures to regulate space activities, including security aspects.*[28]

The EU Council Conclusion on the Space Strategy (2023) emphasises the importance of timely action by Member States, considering hostile space behaviour (such as jamming, manipulation, destruction of space infrastructures and systems).[29]

The ENISA Threat Landscape 2023 identifies ransomware and denial of service threats as the highest threat level, after social engineering, data-related threats, information manipulation, supply chain attacks and malware. The most targeted

[23] Bányász et al. 2022: 9.

[24] European Commission 2023c: 4, 5.

[25] European Commission 2023a: 3

[26] European Union Space Strategy for Security and Defence.

[27] The later interpreted CER Directive and the NIS2 Directive identify the space sector as a critical domain (both as critical infrastructure and essential communication services).

[28] European Commission 2023b: 3.

[29] Council of the European Union 2023e: 6, 7.

sector in 2023 is the public sector (~19%). There is a significant increase in social engineering attacks supported by artificial intelligence in 2023.[30]

The ENISA's *Foresight 2030 Threats* (2023) has a more extended analysis horizon. The report ranks the supply chain attacks (software dependency compromise), disinformation campaigns and digital surveillance authoritarianism[31] in the top three.[32]

The report also identifies other threats that could be considered attractive, such as targeted attacks (e.g. ransomware) against smart devices; attacks on the vulnerability of space-based infrastructure (due to lack of understanding, analysis and control); threats to cross-border ICT providers (single point of failure effects in the case of critical infrastructure, e.g. transport, power grids and industry); and the abuse of artificial intelligence (manipulation of AI algorithms and training data).[33]

The EU Statement on Existing and Potential Threats in the UN Open-Ended Working Group on ICT of 19 December 2023 summarises the most critical cyber threats as:[34]

- attacks on software supply chains (the number of attacks on software supply chains tripled in 2022)
- ransomware attacks (the scale and severity of this attack are increasing, and the risk to essential services and critical national infrastructure may rise to the level of national and international security)
- malicious cyber activity driven by AI-powered software in the long term[35]

The strategy papers presented above demonstrate the need to analyse threats and their effects, and to provide the basis for the necessary response. At the national level, the Hungarian strategies (e.g. National Security Strategy, National Cybersecurity Strategy) – like the EU documents – contain threat statements and risk forecasts and, based on these, high-level security requirements and related tasks. However, due to the strategies' different life cycles and functions, the statements and requirements are not always consistent with each other and the security environment.

The space segment is critical not only for nations involved in spaceflight, therefore, Hungary must also consider the threat of loss of communication channels, communication or navigation equipment in space, which can cause severe disruptions in critical infrastructure or information environments with poor coverage (e.g. military missions and operations).

The new Hungarian approach is straightforward about the threats and risks at the national level. The Act XCIII of 2021 on the coordination of security and defence activities requires a specific risk summary as a decision of the Parliament ["the Principles of Security and Defence Policy" – §22 (1) a)] to create a common base for all strategic level documents.[36]

[30] ENISA 2023c: 4.

[31] The last two threats cannot be considered as pure cyber threats, but rather as complex threats with cyberspace elements.

[32] ENISA 2023b: 2–4.

[33] ENISA 2023b: 6, 7, 10–11.

[34] European External Action Service 2023f.

[35] Otherwise, the AI-powered cyber defences can detect and respond to cyber threats and bolstering security of military networks.

[36] Act XCIII of 2021.

Developments, new solutions to strengthen cybersecurity

The Network and Information Security Directive (NIS 2 Directive) (2022) aims to significantly enhance cybersecurity and establish a standard level of security measures[37] across the EU.

Expands the range of covered entities, creates categories of 'essential' and 'important' for entities in critical sectors, and includes – for the first time – medium-sized service providers.[38]

The Directive requires organisations to carry out regular risk assessments and to take the necessary security measures in line with EU CER[39] Directive and EU DORA[40] (specification for the secure financial sector).[41] Essential or important entities *must submit an incident notification in case of significant incidents within 72 hours,* applying a multi-stage approach.[42]

It requires Member States to establish national Computer Security Incident Response Team(s) (CSIRTs) for incident handling and information sharing, strengthens national competent authorities with additional powers and designates a single point of contact for communication and cooperation at the EU level.

The EU has established a cooperation network (CSIRTs Network), the European Cyber Crisis Liaison Organisation Network (EU-CyCLONe) and the EU NIS 2 Cooperation Group supported by national representatives to ensure effective cooperation. The EU-CyCLONe and the CSIRTs network should have procedural arrangements[43] to avoid overlap and duplication.[44]

Member States *should encourage the development of artificial intelligence and the use of open-source tools,* establish procedures to deal with ransomware and promote the use of encryption techniques.[45]

In parallel with the cybersecurity measures and procedures, Member States shall establish their national cybersecurity strategy within the general criteria of the framework provided by the Directive, including the adoption of policies to promote active cyber protection methods.[46]

The National Cybersecurity Strategies (NCSS) framework developed by ENISA (2020) helps Member States understand their maturity level and assist them in developing their cybersecurity capabilities. The framework has four focus areas: *cybersecurity governance and standards, capacity building and awareness, legislation and regulation* and *cooperation.*[47]

[37] Member States are obliged to implement the requirements into their national legal frameworks by 18 October 2024.

[38] Directive (EU) 2022/2555: 2–3.

[39] CER: Critical Entities Resilience.

[40] DORA: Digital Operational Resilience Act.

[41] Regulation (EU) 2022/2554.

[42] Directive (EU) 2022/2555: 16, 20.

[43] In principle, the EU CyCLON has a crisis management function, while the CSIRTs Network's main task is to support incident response at technical level.

[44] Directive (EU) 2022/2555: 14.

[45] Directive (EU) 2022/2555: 11.

[46] Directive (EU) 2022/2555: 7, 12.

[47] See: www.enisa.europa.eu/topics/national-cyber-security-strategies

The EU Directive on the resilience of critical entities (Critical Entities Resilience Directive – CER) focuses on improving the resilience of critical entities (organisations) as providers of essential services within the EU.[48]

To ensure a comprehensive approach, the Directive requires Member States to develop strategies[49] to support critical entities, integrating existing policies and regulations, considering hybrid threats.[50]

The Directive establishes standard rules for identifying critical entities in essential sectors.[51]

Member States should define significant disruptive impacts and their levels (taking into account negative consequences), designate a *competent authority* to supervise entities and procedures and identify a single point of contact for cross-border cooperation.[52]

Critical entities shall carry out risk analysis[53] concerning the provision of essential services and take *technical, security* and *organisational* measures proportionate to the risks. Critical entities should describe their measures in the *Resilience Plan* (or equivalent document). Each critical entity shall designate a *liaison officer* to the competent authority. Critical entities shall report significantly disruptive incidents to the competent authority within 24 hours. The initial notification shall provide only the strictly necessary information and the presumed reasons.

A Critical Entities Resilience Group composed of representatives of the Member States' competent authorities and of the Commission should be established, which should cooperate with the EU NIS 2 Cooperation Group.[54]

Roepke and Thankey explain[55] that more resilient countries have fewer vulnerabilities as a result of a whole-of-government approach and joint preparation by the public and private sectors. In addition, resilience is an important aspect of deterrence by denial: an attack will not achieve its intended objectives. Mógor and Angyal believe[56] it is important that, during complex exercises conducted in accordance with the requirements of Hungarian legislation, the operating organisations and the competent authorities jointly review the procedures set out in the security plan and the responses to threats.

The proposal for an EU Cyber Solidarity Act (2023) aims to strengthen the EU's cybersecurity capabilities *in the event of significant and large-scale cybersecurity threats and attacks.* The Act describes the detection, preparedness and response functions[57] and consists of three main pillars:

[48] The EU CER Directive has similar logic to the EU NIS 2 Directive.

[49] The Directive does not specify a name for the Strategy ("a strategy for enhancing the resilience of critical entities"), but defines its main aspects. (The Strategy may be a classified document, if necessary.)

[50] Directive (EU) 2022/2557: 2, 14–15.

[51] Energy, transport, banking, financial market infrastructures, health, drinking water, waste water, digital infrastructure, ICT service management (business-to-business), public administration and space.

[52] Directive (EU) 2022/2557: 5–7, 17–18.

[53] The risk assessment shall be reviewed every four years or in case of significant changes (risks, circumstances).

[54] Directive (EU) 2022/2557: 25–26.

[55] Roepke–Thankey 2019: 1.

[56] Mógor–Angyal 2022: 122.

[57] At this stage, these names and titles have only a 'working function' – given that the EU Act is still being developed at the time of writing.

- *European Cybersecurity Shield.* The Shield is not military equipment or a specific hardware-software platform, but a cooperative capability of national competent organisations participating in the EU-level capability voluntarily. The widely interconnected EU entities support the detection of incidents and threats, focus on crisis management and facilitate responses. The planned capability should not overlap with the EU CSIRT Network, the EU CyCLONe,[58] the EU NIS Cooperation Group or other competent national bodies as defined in the EU NIS 2 Directive.[59]
- *Cybersecurity Emergency Mechanism.* The proposal includes a comprehensive emergency mechanism to support critical entities and essential services in high critical sectors. The Mechanism consists of *preparation* (e.g. test of critical important entities in critical infrastructure sectors), reactions and restoration capabilities in case of severe cyberattacks, supported by trusted companies in the framework of Cybersecurity Reserve (e.g. trusted dedicated companies) and common solidarity support provided by national authorities and entities.[60]
- *Cybersecurity Incident Review Mechanism.* This mechanism provides support from ENISA in the event of significant and large-scale cyber-attacks, with *technical review* and *assessment* of incidents at the request of EU bodies or national competent authorities.[61]

The Cybersecurity Support Action (2023) provided by ENISA is a comprehensive set of services to Member States for prevention ('ex-ante') as incident management, response and coordination, and response ('ex-post') as cybersecurity exercises, training and capability assessments.[62]

The NATO Resilience Commitment has a similar methodology for the resilience capabilities of critical infrastructure and services important to NATO operations (including national supporting elements in NATO deployments).[63] In terms of resilience, Jacuch believes[64] that it is important that the baseline requirements are applied to the entire spectrum of crises.

The Alliance identified *Baseline Requirements for National Resilience* in 2016. The seven areas are where specific intent is needed: continuity of government, energy supply, uncontrolled movement of people, food and water resources, mass casualty and disruptive health crises, civil communications systems and transportation systems.[65] NATO created a framework for cooperation to support Allies' national resilience activities, including an annual updating process, consultations, courses and development of assessment criteria and methodologies.

[58] EU Cyber Crisis Liaison Organisation Network.

[59] European Commission 2023f: 23.

[60] European Commission 2023f: 26.

[61] European Commission 2023f: 32.

[62] ENISA 2023a.

[63] NATO 2016a.

[64] Jacuch 2020: 17.

[65] NATO 2016c.

Kádár confirms[66] that the national regulations reflect the basic requirements for NATO resilience, complemented by aspects of preparedness and commitment.[67]

The EU proposal for a Regulation on Cybersecurity Requirements (the Cyber Resilience Act – CRA) aims to establish horizontal cybersecurity requirements for products with digital elements, including connected devices, software and cloud services.

The proposal defines products in the "critical product" category that contain digital elements according to their cybersecurity risk.[68]

Producers must establish *risk management processes* (risk identification and mitigation of cybersecurity risks throughout the product life cycle). Information on exploitable vulnerabilities *must be reported by manufacturers* to the notified authority (organisation) within 24 hours at the latest.[69]

Producers shall develop and maintain *accurate documentation of products* with digital elements to ensure compliance with the requirements for essential products.[70]

Member States must designate a notifying authority to certify quality assurance bodies to the EU and Member States and to *monitor* and *supervise* their activities following EU requirements.[71]

Similarly to EU certification efforts, the *NATO Information Assurance Product Catalogue* (NIAPC) provides up-to-date information on products (hardware, software) to meet NATO operational requirements following NATO strategic requirements for the protection of classified and unclassified information.[72]

The NATO Strengthened Resilience Commitment (2021) confirmed the need to strengthen the resilience of critical infrastructures (land, sea, space and cyberspace) and industry further. *The impact of emerging technologies must be addressed,* and next-generation communication systems must be secured. Investment is needed in robust, flexible and interoperable military capabilities, and supply chains must be secured and diversified. A *whole-of-government approach* is required in order to strengthen resilience capabilities.[73] In connection with cybersecurity, Stoltenberg clearly stated[74] that nations' security is impossible without the private sector, so it is needed "to talk, plan and exercise more together".

The EU Council Recommendation on Critical Infrastructure Resilience was adopted on December 2022. The aim of the Recommendation is to ensure an appropriate, high-level, coordinated and effective EU-wide response to current and future risks to essential services.[75] The Council invited the European Commission to develop

[66] Kádár 2022: 13.
[67] E.g. Act XCIII of 2021 on the coordination of security and defence activities.
[68] European Commission 2022: 36.
[69] European Commission 2022: 38, 40.
[70] European Commission 2022: 47.
[71] European Commission 2022: 49.
[72] See: www.ia.nato.int/NIAPC
[73] NATO 2021b.
[74] Stoltenberg 2023.
[75] The Council of the European Union 2022: 3.

a blueprint[76] to set out the principles for appropriate response to disruptions of critical infrastructure with a significant cross-border impact, in line with other legislation.[77]

The proposed EU Council Recommendation on a Blueprint to coordinate a Union-level response (2023) regulates the exchange of information between EU organisations (institutions, bodies, offices and agencies) and national competent organisations and authorities in case of significant cross-border threats. Nations and EU organisations must activate the appropriate tools if there is a significant disruption of services in six Member States, or a significant disruption of services to six countries, or there is a significant impact on two or more countries and the affected actors agree on the need for coordination at EU level.[78]

The planned Recommendation will regulate *operational, strategic and political cooperation.* States will have to designate a relevant national actor as the point of contact for the use of the Critical Infrastructure Blueprint.[79] The responsible actors recommended *testing the processes of the Critical Infrastructure Blueprint, including exercises at the* EU level with physical and cyber aspects. The results of the tests and the experience of the incidents should be evaluated by the Critical Entities Resilience Group, and nations must prepare a report with the lessons learned to the EU.[80]

In addition to technical responses to complex cyber threats, *the EU Cyber Diplomacy Toolbox* is a solution that enables complex economic and diplomatic responses.

Similarly, *the NATO North Atlantic Council consultation mechanism* can decide on Alliance-level actions and operations, including complex responses to cyber incidents, on *case-by-case basis.*

The proposal for a regulation amending the Cyber Security Act as regards managed security services (2023) creates new requirements in the field of cyber certification of ICT[81] products and services. The EU NIS 2 Directive introduced "managed security services" within the scope of ICT services. Managed security services are also important because service providers can provide (and receive) guarantees on the reliability of a cyber product and services within the framework of the Cybersecurity Emergency Mechanism (including Cybersecurity Reserve), as previously mentioned. Member States should address this regulatory change consistently and include this product in the scope of cyber product certification to avoid fragmentation inside the EU. Following the legislative change, Member States have to implement the change in their cyber product and service certification schemes and processes.[82]

The NATO Cyber Pledge (2016) is another tool to support the national cyber capability development in critical areas. The Pledge is a practical, strategic level

[76] The Council of the European Union 2022: 10.

[77] E.g. counter hybrid threats regulations, CER Directive, NIS2 Directive, 'Cyber Blueprint' (Commission Recommendation 2017/1584 on coordinated response to large scale cybersecurity incidents and crises).

[78] European Commission 2023d: 6, 11.

[79] The contact point should be same as the single point of contact (SPOC) in the CER Directive.

[80] European Commission 2023d: 14.

[81] ICT: Information and Communication Technology.

[82] European Commission 2023e: 5–6.

identification of the main capability development areas[83] for nations with annual self-assessment, national–NATO consultation and alliance-wide common evaluation.[84] Stoltenberg underlined that the Allies have increased their investments in cyber, and enhanced skills and capabilities to implement the national strategies in the NATO Cyber Pledge framework.

The NATO Vilnius Summit Communiqué (2023) states that the Allies restated the enhanced Cyber Defence Pledge with critical infrastructures.[85]

The NATO Madrid Summit Declaration (2022) announced that the Allies have decided to establish a virtual rapid response cyber capability, supported by nations on voluntary basis, to respond to significant malicious cyber activity.[86]

The Vilnius Summit Communiqué (2023) states that NATO has established the Virtual Cyber Incident Support Capability (VCISC) as a new solution to assist nations in responding to significant malicious cyber activity.[87]

Bányász et al. conclude[88] that the Allies are responsible for their cyber defences. The NATO provides a platform for consultation, exchange of information and best practice.

The International Counter Ransomware Initiative 2023 Joint Statement summarises the efforts of the international community in the last year:

- capability development (to disrupt attackers and the infrastructure used to carry out their attacks): mentoring and tactical training for new members; launching a project to use artificial intelligence in the fight against ransomware
- information sharing: developing a specific platform and CRI website to support member cooperation; encouraging reporting of ransomware incidents to relevant government authorities
- operations: drafting a policy statement that member governments will not pay ransoms; sharing data from illegal wallets; providing mutual assistance[89]

Members issued a joint statement against ransomware payments. Organisations controlled by member governments do not pay ransomware because payment:

- does not guarantee the end of the incident or the removal of malware from systems
- encourages criminals to continue and expand their activities
- provides funds for criminals to use for illegal activities
- does not guarantee the recovery of data[90]

[83] Capabilities to defend our national infrastructures and networks; adequate resources, interactions (cooperation, exchange of best practices); understanding of cyber threats (and information sharing), skills and awareness, cyber education, training and exercises and bolster security of national systems upon which NATO depends.

[84] NATO 2016b.

[85] NATO 2023.

[86] NATO 2022a.

[87] NATO 2023.

[88] Bányász et al. 2022: 18.

[89] ICRI 2023b.

[90] ICRI 2023a.

The EU proposal for a regulation on artificial intelligence (2021) addresses the risks associated with the use of this technology. The planned act identifies the prohibited AI practices[91] and establishes the classification rules of the high-risk AI systems,[92] as well as the requirement to establish and maintain a risk management system.[93] In addition, there are other requirements (e.g. data governance, documentation, event logs, cybersecurity) and obligations (e.g. providers, users, distributors).[94] Each Member State shall designate or establish a notifying authority to supervise and monitor conformity assessment bodies.[95]

The various aspects, functions and high-level risks of the use of artificial intelligence and finally, the possible, unpredictable effects, create a completely uncertain, foggy environment that slows down the pace of regulation. Recognising the difficulties, it is positive that – as a new step in regulation – the EU Parliament and the Council have reached a political consensus on the main issues of the proposal in late 2023, so that the planned Act can realistically be expected in 2024.[96]

The European Declaration on Quantum Technologies (Quantum Pact) (2023) recognises the strategic importance of quantum technologies based on the statements of the European Economic Security Strategy and the Commission Recommendation, as mentioned earlier in this paper. To protect the strategic assets, interests and security of the EU and to avoid strategic dependence on non-EU sources, it is necessary to build up its own research and development capabilities in the main areas of quantum technologies: *quantum computing and simulation, quantum communication, quantum sensing* and *metrology.*

Member States will coordinate their efforts in European national and regional research and development programmes and initiatives in quantum technologies. They will encourage companies to invest in quantum technologies to support the EU's economic security and technological autonomy.

Members will identify the necessary skills and training needs and undertake the activities required for a deeper understanding of the social and economic implications and challenges of quantum technologies.[97]

The European Cybersecurity Competence Centre has raised a specific quantum area in its Strategic Agenda (2023), the post-quantum cryptography. The EU still needs to *have a strategy-level document dedicated to these issues,* but the secure use of post-quantum cryptography requires close attention (e.g. development, implementation and assurance). The Agenda underlined the importance of risk analysis with prioritisation; on this basis, a strategy for using post-quantum cryptography should be developed.[98]

The Belgian Presidency has identified the main priorities in cybersecurity: "active cyber protection" (establish a common approach to prevent, detect, monitor and

[91] European Commission 2021: 43–45.
[92] European Commission 2021: 45–46.
[93] European Commission 2021: 46–48.
[94] European Commission 2021: 52–58.
[95] European Commission 2021: 58.
[96] European Parliament 2023b.
[97] European Union 2023c: 2–3.
[98] European Cybersecurity Competence Centre and Network 2023: 9, 10.

mitigate cyber incidents), trust in the digital domain and enhancing cyber resilience (including space infrastructure).

The Presidency plans to *finalise the Cyber Solidarity Act* and review *the EU's Cyber Defence Policy* and institutional landscape (gap identification).[99]

The report of the UN Open-ended Working Group on Security (2022) noted the importance of understanding national perspectives on the applicability of international law. States are invited on voluntary basis to share their national views and positions on international law in the use of ICTs.[100]

Generally, red lines are largely undefined and untested, and the threshold indicators – scale, effects, circumstances and motivations – are even more obscure in cyber domain as Pedersen states,[101] so publishing the national point of view is an effective tool for the next generation of international standards and norms.

According to Stoltenberg's speech,[102] the cyberspace should not be a "Wild West" free-for-all and "all Allies agree that fundamental rights and international law apply".

General considerations

Based on the observations of the study, it is possible to formulate general guidelines that can help to develop specific regulations at the national level. This is necessary because there is only one Hungarian cybersecurity framework (organisations, regulations, external interfaces, etc.), which must be capable of different (e.g. UN, EU, NATO) international cooperations.

Emerging threats. The increase in cyber threats (number, effectiveness and complexity), their focus on critical infrastructure and cyber infrastructure and the presence of hybrid operations are highlighted from both the EU and NATO perspectives.

Emerging and Disruptive Technologies (EDT). In addition to the increasing number of technical and regulatory question marks, the emergence of new threats and risks in the EDT and the expression of the need to address them is a growing international trend.

Complexity and interdependence. In support of the strategic objectives for the enhancement of the level of security in cyberspace, an increasing number of actions can be identified horizontally. Information systems, services and tools are an indispensable part of social and economic processes and critical infrastructures, so that their compromise can lead to further failures including cross-border impacts. Security issues must be enforced throughout the lifecycle of services and products (e.g. supply chain security, AI development and operation).

Risk based approach. The changing security environment requires ongoing risk-based, intelligence-driven security policies and governance.

Evolution and hierarchy. The sources presented justify the continuous evolution of cyber protection mechanisms and processes and the logic of sequential steps

[99] Centre for Cybersecurity Belgium 2023.
[100] United Nations 2022: 11.
[101] Pedersen 2023: 63.
[102] Stoltenberg 2022.

(including periodic review and reinforcement actions). The strategic, operational and technical structure is also clearly identifiable.[103] A multi-layered security structure and cooperation framework is necessary for the effective and fast international and national responses.

Solidarity and assistance. In addition to developing technical cyber protection mechanisms, various forms of solidarity and assistance (national, regional and EU-NATO) are strongly emerging. In addition to solidarity, operational and technical cooperation is needed to identify and respond effectively to cross-border impacts.

Sovereignty and self-defence. Effective resilience and self-defence – including countering the harmful effects of national and international dependencies – in the case of critical infrastructure protection and cybersecurity are essentially national responsibilities, complemented by EU and Alliance assistance.

International efforts. International cooperation frameworks (e.g. ransomware, artificial intelligence and quantum) are being developed to study important issues and find solutions (e.g. gap analysis, research, methods and procedures, education, information and best practices exchange, tests).

Taking into account the above guidelines, national frameworks and interfaces for participation in international and national processes should be continuously ensured.

National laws and regulations need to be managed in a complex manner along the above lines, as fragmentation of regulation can provide an unnecessary attack surface (lawfare effects) to achieve the objectives of the adversary.

National impacts

The EU NIS 2 and EU CER Directives directly impact Hungary. In the area of cybersecurity, the two existing Hungarian strategies[104] should be replaced by a modern national cybersecurity strategy. According to Bányász et al.,[105] the two cyberspace strategies are partly complementary and partly contradictory. In the area of critical infrastructure, a *national strategy should be adopted*, which has yet to be done in Hungary.

In both areas, laws and supporting directives need to be revised and updated to ensure EU compatibility. A recent example is the *revision of the national requirements for the security of electronic information systems*–with public consultation (security classification and security measures). [106]

The proposed Cyber Resilience Act will provide a broad EU basis for common risk-based requirements for cybersecurity certification of digital products (hardware, software) and support citizens' security awareness. The planned new EU requirement for mandatory certification of managed security services will *directly impact Hungarian*

[103] Ad-hoc decisions cannot establish and maintain strategic, stable states or processes even in cyberspace.

[104] 1139/2013 (III. 21.) Government Decision on Hungary National Cyber Security Strategy and 1838/2018 of 28 December 2018 Government Decision on Hungary Strategy for the Security of Network and Information Systems.

[105] Bányász et al. 2022: 4.

[106] Magyarország Kormánya 2023.

cyber product certification laws[107] and procedures in both commercial and military cases. *The NATO Resilience Commitment* and the *NATO Cyber Pledge* also aim to support the development of national capabilities analogous to the requirements of the EU. NATO and the EU share a common approach to critical infrastructure and cybersecurity, and there is close cooperation in a number of areas (exercises, joint working groups and forums, technical agreements).

The planned new EU Cyber Solidarity Capabilities will also provide technical support to Member States (e.g. incident management and recovery support, international cooperation) and provide an opportunity for industry to offer capabilities (e.g. Cyber Reserve System). The Hungarian Electronic Information Security Early Warning System complements the national incident management system by collecting one-way data flows from sensors of protected information systems, providing an enhanced protection solution.[108] *The planned EU Cyber Shield will offer possible cooperation,* depending on details in the future.

The upcoming EU Act on Artificial Intelligence (AI) will *directly apply in Hungary,* so preparing for its application and considering the potential threats is an urgent task.

The threat of ransomware has increased over the years. Following the international ICR initiative and studying the solutions provided by different entities and nations is useful. Of course, the best solution *would be for Hungary to join the initiative.*

The EU Quantum Pact is a cooperation for developing future capabilities of similar importance as artificial intelligence, of which Hungary is a member. This will provide access to joint research results and *the possibility of involving Hungarian companies and research institutions in projects.* The predictable new EU quantum requirements may lead to *direct changes in the existing Hungarian regulations* on the security of information systems.[109]

The recommendation of the UN Working Group on the applicability of international law in Cyberspace suggests that the expression of national positions is a useful process to support international cooperation. Hungary has yet to make such a declaration,[110] so it *would be useful to define the Hungarian position* within the framework of the new strategies (e.g. self-defence, the Hungarian concept of national sovereignty in cyberspace).

The promotion of the development of active cyber protection capabilities and the *revision of the EU's Cyber Defence Policy,* as indicated by the Belgian EU Presidency, also *represent new challenges for Hungary*.

Conclusion

Cybersecurity issues, once simplified to a primarily technical level, are now becoming more complex and sophisticated as the range of threats expands.

[107] Act XXIII of 2023.

[108] Government Decree 214/2020 (V. 18.).

[109] Act L of 2013, 22/F-H. §.

[110] There is no internationally agreed form of national positions, and the publication of the issues is usually straightforward (mainly in the form of a position paper).

The EU and NATO cybersecurity frameworks are constantly evolving, and processes and organisational relationships lead to increasingly complex defence mechanisms.

EU and NATO policies and programmes aim to support the development of national capabilities, improve coordination at the EU and NATO levels and stimulate cooperation and mutual support among nations.

The article describes several EU and NATO initiatives and requirements that will need developing or modifying national laws and procedures. These changes will impact Hungary's cybersecurity framework and capabilities and require revisions and national regulation updates.

The boundary between civil and military cyberspace (or physical and cyber dimensions) is sometimes foggy and mysterious. From another perspective, the military is part of national security, so the presented new requirements will affect military capabilities, cooperation and coordination issues at both national and international levels, but this may already be the subject of a future article.

Digitalisation is not a closed issue, so new needs and solutions will create new threats, needing new security requirements, processes and protection mechanisms to balance them. For this reason, the cybersecurity outlook and snapshot presented in this article will show significant differences and evolution in the coming years.

Finally, many thanks to friends and colleagues (both civilian and military) who contributed their opinions and suggestions to this article.

(The research for this publication was completed on 23 February 2024.)

References

Bányász, Péter – Krasznay, Csaba – Tóth, András (2022): *A kibervédelem szakpolitikai szintjének helyzete és kihívásai Magyarországon, az EU-ban és a NATO-ban* [Situation and Challenges at the Policy Level of Cyber Defence in Hungary, the EU and NATO]. Military and Intelligence Cyber Security Research Paper 2022/8.

Bihaly, Barbara (2021): A kibervédelem szerepe az Európai Unió közös biztonsági és védelmi politikájában [The Role of Cyber Defence in the European Union's Common Security and Defence Policy]. *Hadtudományi Szemle,* 14(3), 45–55. Online: https://doi.org/10.32563/hsz.2021.3.4

Centre for Cybersecurity Belgium (2023): *Cybersecurity Priorities in the Upcoming Belgian Presidency Agenda.* Online: https://ccb.belgium.be/en/news/cybersecurity-priorities-upcoming-belgian-eu-presidency-agenda

The Council of the European Union (2022): *Council Recommendation of 8 December 2022 on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure.* 2023/C 20/01. Online: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023H0120(01)

The Council of the European Union (2023): Council Conclusions on the EU Space Strategy for Security and Defence. 14512/23. Online: https://data.consilium.europa.eu/doc/document/ST-14512-2023-INIT/en/pdf

ENISA (2023a): *Cybersecurity Support Action.* Online: www.enisa.europa.eu/publications/cybersecurity-support-action

ENISA (2023b): *Foresight 2030 Threats.* Online: www.enisa.europa.eu/publications/foresight-2030-threats

ENISA (2023c): *ENISA Threat Landscape 2023* (July 2022 to June 2023). Online: www.enisa.europa.eu/publications/enisa-threat-landscape-2023

European Commission (2020): *Joint Communication to the European Parliament and the Council. The EU's Cybersecurity Strategy for the Digital Decade.* JOIN(2020) 18 final. Online: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52020JC0018

European Commission (2021): *Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts.* COM(2021) 206 final. Online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206

European Commission (2022): *Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020.* COM/2022/454 final. Online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52022PC0454

European Commission (2023a): *Commission Recommendation of 03 October 2023 on critical technology areas for the EU's economic security for further risk assessment with Member States.* C(2023) 6689 final. Online: https://defence-industry-space.ec.europa.eu/commission-recommendation-03-october-2023-critical-technology-areas-eus-economic-security-further_en

European Commission (2023b): *Joint Communication to the European Parliament and the Council. European Union Space Strategy for Security and Defence.* JOIN(2023) 9 final. Online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023JC0009

European Commission (2023c): *Joint Communication to the European Parliament, the European Council and the Council on "European Economic Security Strategy".* JOIN(2023) 20 final. Online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023JC0020

European Commission (2023d): *Proposal for a Council Recommendation on a Blueprint to coordinate a Union-level response to disruptions of critical infrastructure with significant cross-border relevance.* Online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023DC0526

European Commission (2023e): *Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2019/881 as regards managed security services.* COM(2023) 208 final. Online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2023%3A208%3AFIN

European Commission (2023f): *Proposal for a Regulation of the European Parliament and of the Council Laying Down Measures to Strengthen Solidarity and Capacities in the Union to Detect, Prepare for and Respond to Cybersecurity Threats and Incidents.* COM(2023) 209 final. Online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023PC0209

European Cybersecurity Competence Centre and Network (2023): *Strategic Agenda.* Online: https://cybersecurity-centre.europa.eu/strategic-agenda_en

European Parliament (2023b): *Artificial Intelligence Act: Deal on Comprehensive Rules for Trustworthy AI.* Online: www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai

European Union (2023c): *European Declaration on Quantum Technologies.* Online: https://ec.europa.eu/newsroom/dae/redirection/document/100585

European Union External Action (2022): *A Strategic Compass for Security and Defence. For a European Union that protects its citizens, values and interests and contributes to international peace and security.* Brussels, 21 March 2022. Online: www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf

European External Action Service (2023): *EU Statement – UN Open-Ended Working Group on ICT: Existing and Potential Threats.* Online: www.eeas.europa.eu/delegations/un-new-york/eu-statement-–-un-open-ended-working-group-ict-existing-and-potential-threats_en

ICRI (2023a): *CRI Joint Statement on Ransomware Payments* (2 November 2023). Online: www.gov.uk/government/publications/cri-joint-statement-on-ransomware-payments/cri-joint-statement-on-ransomware-payments

ICRI (2023b): *International Counter Ransomware Initiative 2023 Joint Statement* (1 November 2023). Online: www.whitehouse.gov/briefing-room/statements-releases/2023/11/01/international-counter-ransomware-initiative-2023-joint-statement/

Jacuch, Andrzej (2020): Countering Hybrid Threats: Resilience in the EU and NATO's Strategies. *The Copernicus Journal of Political Studies,* (1), 5–26. Online: https://doi.org/10.12775/CJPS.2020.001

Kádár, Pál (2022): *A kibertér és a kibertér műveleti képességek jelentősége a védelmi és biztonsági tevékenységek összehangolásában* [The Importance of Cyberspace and Cyberspace Operational Capabilities in Improving Coordination of Defence and Security Activities]. Military and Intelligence CyberSecurity Research Paper 2022/7.

Kersánszky, Tamás (2022): The Burden of Cyber Defense in the Common Security and Defence Policy of the EU. *Safety and Security Sciences Review,* 4(4), 69–79.

Kovács, László (2018): Cyber Security Policy and Strategy in the European Union and NATO. *Land Forces Academy Review,* 23(1), 16–24. Online: https://doi.org/10.2478/raft-2018-0002

Kovács, László (2020): A kiberbiztonság és a kiberműveletek megjelenése Magyarország új Nemzeti Biztonsági Stratégiájában [The Appearance of Cybersecurity and Cyber Operations in the New National Security Strategy of Hungary]. *Honvédségi Szemle,* 148(5), 3–18. Online: https://doi.org/10.35926/HSZ.2020.5.1

Magyarország Kormánya (2023): *Biztonsági osztályba sorolás és alkalmazandó védelmi intézkedések min. rendelet.* Online: https://kormany.hu/dokumentumtar/biztonsagi-osztalyba-sorolas-es-alkalmazando-vedelmi-intezkedesek-min-rendelet

Mógor, Judit – Angyal, István (2022): A létfontosságú rendszerek védelmére vonatkozó szabályozás fejlesztése [Development of the Regulations of the Critical Infrastructure Protection]. *Scientia et Securitas,* 3(2), 118–125. Online: https://doi.org/10.1556/112.2022.00102

NATO (2016a): *Commitment to Enhance Resilience.* Online: www.nato.int/cps/en/natohq/official_texts_133180.htm

NATO (2016b): *Cyber Defence Pledge.* Online: www.nato.int/cps/en/natohq/official_texts_133177.htm

NATO (2016c): *Resilience, Civil Preparedness and Article 3.* Online: www.nato.int/cps/en/natohq/topics_132722.htm

NATO (2021a): Cyber Defence. Retrieved 02 14, 2024, from www.nato.int/cps/en/natohq/topics_78170.htm

NATO (2021b): *Strengthened Resilience Commitment.* Online: www.nato.int/cps/en/natohq/official_texts_185340.htm

NATO (2022a): *Madrid Summit Declaration.* Online: www.nato.int/cps/en/natohq / official_texts_196951.htm

NATO (2022b): *NATO 2022 Strategic Concept.* Online: www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf

NATO (2023): *Vilnius Summit Communiqué.* Online: www.nato.int/cps/en/natohq/official_texts_217320.htm

Novák-Varró, Virág (2021): Az „ellenálló képesség", mint a békeépítés eszköze [Resilience as a Tool of Peacebuilding]. *Hadtudomány,* (3), 32–43. Online: https://doi.org/10.17047/HADTUD.2021.31.3.32

Pedersen, Torbjørn (2023): A Small State's Cyber Posture: Deterrence by Punishment and Beyond *Scandinavian Journal of Military Studies,* 6(1), 58–68. Online: https://doi.org/10.31374/sjms.191

Roepke, Wolf-Diether – Thankey, Hasit (2019): The First Line of Defence. *The Three Swords Magazine,* 34/2019. Online: www.jwc.nato.int/images/stories/_news_items_/2019/three-swords/ResilienceTotalDef.pdf

Stoltenberg, Jens (2022): *Keynote address by NATO Secretary General Jens Stoltenberg at the NATO Cyber Defence Pledge Conference in Italy.* Online: www.nato.int/cps/en/natohq/opinions_208925.htm

Stoltenberg, Jens (2023): *Speech by NATO Secretary General Jens Stoltenberg at the first annual NATO Cyber Defence Conference.* Online: www.nato.int/cps/en/natohq/opinions_219806.htm

Szenes, Zoltán (2021): A hibrid fenyegetések elleni szakpolitika Magyarországon [Governmental Policy against Hybrid Threats in Hungary]. *Hadtudomány,* 31(4), 39–56. Online: https://doi.org/10.17047/HADTUD.2021.31.4.39

Szenes, Zoltán (2022): Elrettentés és védelem: a NATO új haderőmodellje [Deterrence and Defence: The New NATO Force Model]. *Hadtudomány,* 32(2), 3–17. Online: https://doi.org/10.17047/HADTUD.2022.32.2.3

United Nations (2022): *Report of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025.* A/77/275, 8 August 2022.

Legal sources

1139/2013 (III. 21.) Government Decision on the National Cyber Security Strategy of Hungary

1838/2018 (XII. 28.) Government Decision on the Strategy for the security of network and information systems in Hungary

Act L of 2013 on Electronic information security of state and municipal bodies

Act XCIII of 2021 on the coordination of security and defence activities

Act XXIII of 2023 on cyber certification and cybersecurity authority

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance). Online: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555

Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. Online: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2557

Government Decree 214/2020 (V. 18.) on the Electronic Information Security Early Warning System

Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (Text with EEA relevance) Online: https://eur-lex.europa.eu/eli/reg/2022/2554/oj