Journal of Electrical Engineering and Information Technologies, Vol. **9,** No. 1, pp. 51–61 (2024)
Article 219
In print: ISSN 2545–4250
Received: May 7, 2024
On line: ISSN 2545–4269
Accepted: May 30, 2024
UDC: 004.491.056:34.05(4-672ЕУ:497.7)
https://doi.org/10.51466/JEEIT2491219051a

Professional paper

CYBER SECURITY LEGAL FRAMEWORK WITH SPECIAL FOCUS ON NIS2 AND N. MACEDONIA

Valentina Angelkoska[1], Ivo Paunovski[2]

[1] *"Ss. Cyril and Methodius" University in Skopje, Faculty of Economics, Skopje, N. Macedonia*
[2] *A1 Macedonia, Skopje, N. Macedonia*
angelkoskavalentina2@gmail.com

A b s t r a c t: The digitization trend and the complex geopolitical situation result in an increased number of cyber attacks worldwide. The countries of the Western Balkans, including N. Macedonia, are no exception to this trend. The subjects of the cyber attacks are the critical infrastructure and data privacy of public and private companies. One of the major issues that N. Macedonia is facing in the domain of cyber security is the lack of an effective legislative framework that will be harmonized with the legislative frameworks of the EU member states. This paper provides an overview of European legislation with a special focus on NIS2 Directive and the actions that regulated companies should undertake in order to meet the requirements of this directive. Apart from an overview of the Macedonian cyber security related legislation, this paper also provides appropriate recommendations for governments and key stakeholders about cyberspace and critical infrastructure protection.

Key words: critical infrastructure; cyber attacks; NIS2 Directive; strategy

ПРАВНА РАМКА ЗА КИБЕР БЕЗБЕДНОСТ СО ПОСЕБЕН ФОКУС НА ДИРЕКТИВАТА NIS2 И С. МАКЕДОНИЈА

А п с т р а к т: Трендот на дигитализација во рамките на општеството и сложената геополитичка ситуација резултираа со пораст на бројот на кибер напади во светски рамки. Земјите од Западен Балкан, вклучително и С. Македонија, не се исклучок од ова правило. Предмет на овие кибер напади се критичната инфраструктура и приватноста на податоците на јавните и приватните компании. Едно од главните прашања со кои се соочува С. Македонија во доменот на кибер-безбедноста е немањето на ефективна законодавна рамка усогласена со законските рамки на земјите членки на ЕУ. Во овој труд е даден приказ на европската легислатива со специјален фокус на Директивата NIS2 и на активностите што регулираните компании треба да ги преземат за да ги исполнат барањата од оваа директива. Освен преглед на македонската легислатива во доменот на кибер-безбедноста, овој труд дава и соодветни препораки со цел подигнување на нивото на безбедноста на критичната инфраструктура.

Клучни зборови: кибер-напади; критична инфраструктура; Ддиректива NIS2; стратегија

1. INTRODUCTION

The number of connected devices on the Internet in EU in 2022 is estimated to be almost 2.7 billion [1]. About 440 (four hundred and forty) million inhabitants live within the European Union, and 90% of them own a smartphone, a personal computer and an Internet connection. On top of it, nearly 95% of companies and public authorities are also connected to the Internet.

The digital revolution and its use by governments, people, private and public enterprises, criminal groups and non-state actors, have increases the exposure to cyber risks. It is estimated that every 40 seconds, companies, and public bodies are victim of a cyber-attack. The World Economic Forum claims

that cyber attacks and cyber warfare are the most serious threats concerning cyberspace. According to [2], the most prevalent violations in cyberspace have been fake news during the Covid-19 pandemic, information security breaches, propaganda, threats, and hate speech. Recently, a large number of cyber-attacks on state institutions and critical infrastructure have been published in the media. Therefore, cyber attacks are no longer seen only as an IT problem but also as a social problem [3]. For example, recently the Irish healthcare system was the target of a ransomware attack that disrupted the operation of the healthcare system. The victim of a cyber attack was also the largest gas distributor in US, due to which the gas distribution in 8 (eight) American states was disrupted for a certain period of time.

Cyber adversaries' level of sophistication, persistence, and technical capability to attack the systems that support critical infrastructure is on the rise in Western Balkans countries as well. In the last few years, companies and state institutions in Macedonia are also frequent targets of cyber attacks. We have been witnesses of a successful cyber attacks on many private companies, banks and also large state institutions like Health Insurance Fund, the Agency for Electronic Communications, the Agency for Real Estate Cadaster and MEPSO. Most of these attacks originate outside the territory of the Western Balkans. The consequences of successful cyber attacks, apart from the damage to the company itself, directly and/or indirectly affected other companies and natural persons. Therefore, it is critical for private companies and Macedonian government to be aware of such violations in order to better understand the need for investment in cyber security expertise.

Taking any protective measures is associated with the generation of costs. Bearing in mind that generation of profit is built in the core of the existence of any private company, making any business decisions are made based on the analysis of costs and potential profit [4]. On the cost side, only the costs related to the remediation of damage caused by the cyber attack and estimation of the damage to the reputation of the brand are usually calculated. Companies typically do not take into account the impact of a cyber attack on other businesses or society itself. Failure or unwillingness to calculate these costs contributes to inadequate investment in network and information system security. Compensation for damage caused by the violation of legal rights of other businesses that are closely related to the affected company are ineffective [5]. Therefore, European Union introduced a series of regulations that require companies to introduce certain standards and norms related to cyber protection [6].

2. EU CYBER SECURITY LEGAL FRAMEWORK

The origins of cyber security legislation date back to 2008, when the first draft version of European Critical Infrastructure Directive (ECI) was prepared, aimed at transport and energy infrastructure. This directive represents a basis for future texts in terms of defining a common approach, although the risks related to cybersecurity were not part of this directive.

The cornerstone of the common cyber security policy was born in 2013 with the adoption of the first EU Cyber Security Strategy (EUCSS) [7]. The EUCSS is the first official document published by the EU where the term "cyber security" is used for the first time. According to this strategy, the EU has instructed each member state to implement a National Computer Emergency Response Team (CERT) as a competent cyber security authority that will represent the country in discussions at European level.

In 2016, the Network and Information Systems directive (NIS) was adopted [8]. This directive applied to Digital Service Providers (DSP) and Operators of Essential Services (OES). The scope of the NIS directive was applicable to 7 (seven) different sectors. The aim of this directive was to ensure a high and common level of security of EU networks and information systems. The cyber-resilient program was developed based on three main pillars:

- Improving national cyber security capabilities;
- Building cooperation at EU level;
- Promoting a culture of risk management and incident reporting.

In accordance with the NIS directive, each of the member states created a NIS Cooperation Group. The work of these NIS groups is coordinated by European Union Agency for Cybersecurity – ENISA (www.enisa.europa.eu). The main duty of ENISA is achieving a high common level of cyber security across Europe. Also, ENISA contributes to EU cyber policy, enhances the trustworthiness of ICT products, services, and processes with the introduction of cyber security certification schemes. The NIS directive showed its limitations during the "Covid-19" crisis, given that this period was represented by rapid digital transformation of the society. Therefore, the EU Commission decided to work on the NIS2 directive which was adopted in 2023 [9].

Maybe the most significant step in regards of European legislation is the adoption of the GDPR (General Data Protection Regulation), a regulation that refers to the protection of personal data [10]. The GDPR regulation adopted in 2016 is the first European regulation that focuses on the unification of legislation among all EU member states when it comes to the protection of users' personal data and establishes sanctions in case of non-compliance with such obligations. In accordance with the GDPR regulation, the Digital Services Act (DSA) [11] was adopted in 2022. With this law, all digital companies and online intermediaries offering their services in the EU Single Market, regardless of whether they are established in the EU or outside it, must comply with obligations related to transparency and cooperation with national authorities. In case of non-compliance, fines and sanctions can amount to up to 6% of the platform's annual turnover. Since the Digital Services Act (DSA) had certain shortcomings, in 2022 the Data Governance Act (DGA) [12] was adopted. The objective of this act was to create a single European data market and the promotion of confidential data sharing. This act is generally focused on specific sectors such as health, energy, transport, supply chain. It is important to note that with this act the use of artificial intelligence (AI) begins to be regulated for the first time. The main purpose of enacting the DGA is to give some power to small and medium-sized enterprises compared to the power that digital leaders have given that it addresses the need to seek and give consent by the individuals in case their personal data needs to be processed. This act also applies to other data holders who should now allow the use of non-personal data for the purposes of general interest, i.e., scientific research or improving the public services without any compensation. What is particularly important to note here is that whenever it comes to data transfer it is necessary to ensure compliance with the GDPR regulation.

In order to speed up the digitization process in EU, in 2014 the eIDAS regulation [13] was passed which enabled EU citizens to use a national electronic identification (eID) scheme, such as ItsMe in Belgium, to access public services online not only in Belgium but also in other countries within the European Economic Area. In 2021, the European Commission introduced eIDAS 2.0 which enabled the addition of digital wallets to eIDAS. Digital wallets are applications and services that enable secure digital identity management.

Within the framework of the banking and financial sector, the EU adopted two directives:

- Payment Services Directive 2 (PSD2) [14] has established guidelines on major incident reporting, setting out the criteria, thresholds, and methodology to be used by payment service providers (PSP) to determine whether an operational or security incident should be considered major or not and accordingly defined the procedure for notification of the Member State's competent authority.
- Digital Operational Resilience Act (DORA**)** [15], which defines uniform requirements for the security of the networks and information systems of companies and organizations active in the financial sector as well as critical the third parties that provide services related to ICTs.

After the adoption of EUCSS in 2013, the second cornerstone of the EU cyber security legislation was related to the introduction of EU Cybersecurity Act (EU CS Act) [16] in 2019, bringing forward awareness on the new needs in terms of cyber security, resilience, and cooperation in the EU. EU CS act is having two focus points:

- The European Certification Framework providing companies set of rules, technical requirements, standards, and procedures;
- Strengthening the European Network Information Security Agency (ENISA), European Union Agency for Cyber security.

In December 2020, the EU published its second Cyber Security Strategy (EUCSS). This new strategy was adopted in order to provide guarantees for a global and open Internet by implementing strong safeguards in case of cyber security risks. This strategy today is probably best known for the announcement of NIS2 Directive.

From artificial intelligence regulation point of view, the Law on Artificial Intelligence (AI Act) was adopted, which ensures the introduction of a common legal framework that applies to all types of systems and to all sectors except the military sector. The AI Act banned unacceptable practices, such as manipulating people through subliminal techniques or remote real-time biometric identification. The latest regulation passed by the EU is the Cyber Resilient Act (CRA). The CRA aims to improve transparency in the security domain of hardware and software products by introducing a coherent cyber security framework within which hardware and software manufacturers remain accountable for cyber security throughout the entire lifecycle of their products. The CRA aims to complement the AI Act, the CSA and the NIS2 Directive.

In recent years, intensive activity can be observed within the framework of EU legislation aimed at raising the level of cyber security in EU member states. Table 1 shows the time line of EU cyber security legal framework while the Figure 1 represent a simplified view of the overall legislation produced by the EU. In the next part of this paper we will look a little more at what improvements NIS2 offers in relation to the NIS Directive and what companies need to do to be ready when this directive comes into force.

T a b l e 1

Timeframe of EU cyber security legal framework

Year	Act
2013	EUCSS
2014	eIDAS
2015	Digital Single Market
2016	GDPR + NIS
2019	Cyber Security Act
2020	DSA + EUCSS
2021	AI Act
2022	DG Act + CR Act
2023	NIS2 Act

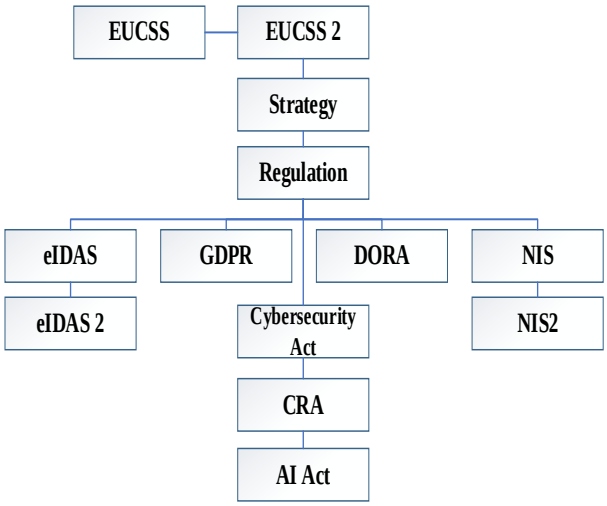

Fig. 1. EU Cyber Security Legislation – graphic display.

3. EVOLUTION FROM NIS TO NIS2

The NIS and NIS2 directives aim to strengthen the security of networks and information systems. In terms of the general scope of both directives, networks and information systems mean all electronic communication networks, equipment that enables digital data processing and data itself that is digitally processed (Article 4, paragraph 1).

The aim of the NIS2 Directive is to remove the shortcomings of the NIS and adapt it to the current needs. The NIS Directive applied to digital service providers (DSP) and operators of essential services (OES), in 7 (seven) different sectors including that of health, energy, transport, digital infrastructure and water supply. The NIS Directive left the discretionary right to the member states to identify the providers or operators of essential services, which introduces legal uncertainty, especially from the point of view of companies that have their operations in several countries. In order to overcome this shortcoming, the NIS2 Directive expands the scope of application by adding new sectors based on the degree of digitization and their significance for the economy and society itself. This means that NIS2 removes the distinction between DSP and OES by introducing two new categories (operators of essential services (OES) and important entities) and the size of a company that will be subject to different supervision. OES are companies that provide so-called critical services, that is, services that are essential for the functioning of society and the economy as indicated in Table 2. OES companies must comply with the NIS2 Directive regardless of their size. The group of important entities includes large or medium-sized enterprises (large enterprises includes companies that have over 250 employees or more than 50 million euros in annual revenues). Medium-sized enterprises are enterprises that have between 50 and 250 employees or an annual income of more than 10–50 million euros) that operate in the sectors listed in the following table. By introducing a definition of company size, the scope of the NIS2 Directive practically covers all medium and large enterprises in the selected sectors. Member States will also be able to include in the scope smaller entities but with a high security profile.

It should be emphasized that in comparison with NIS Directive, the proposed NIS2 Directive includes numerous examples of organizational and technical measures to improve the security of information systems. The NIS2 Directive, among other things, adds new requirements for 5 (five) primary areas (management, risk management, supervision, reporting and business continuity).

T a b l e 2

Description of OES and important entities

Operators of essential services (OES)	Important entities
Energy – electricity, heating and cooling, oil, gas, hydrogen	**Postal and courier services**
Transport – air, rail, water, road	**Waste management**
Banking & Financial market infrastructures	**Production, processing and distribution of food –** food businesses which are engaged in wholesale distribution and industrial production and processing
Health – Healthcare providers, laboratories, research and development of medicinal products, manufacturers of basic pharmaceutical products and preparations, manufacturers of medical devices considered to be critical during a public health emergency	**Manufacture, production and distribution of chemicals –** undertakings carrying out the manufacture of substances and the distribution of substances or mixtures, and undertakings carrying out the production of articles from substances or mixtures
Drinking water – suppliers and distributors of water intended for human consumption	**Manufacturing** – manufacture of medical devices and in vitro diagnostic medical devices, manufacture of computer, electronic and optical products, manufacture of electrical equipment, manufacture of machinery and equipment, manufacture of motor vehicles, trailers and semi–trailers, manufacture of other transport equipment
Waste water – collectors, disposers, and treaters of urban, domestic, or industrial waste water	**Digital providers –** providers of online marketplaces, providers of online search engines, providers of social networking services platforms
Digital infrastructure – Internet exchange point providers; DNS service providers; TLD name registries; cloud computing service providers; data center service providers; content delivery network providers; trust service providers; providers of public electronic communications networks; providers of publicly available electronic communication service	**Research organizations**
ICT service management – (business–to–business) managed service providers (msps), managed security service providers (MSSPs)	
Public administration – public administration entities of central governments and at the regional level	
Space – operators of ground–based infrastructure owned, managed, and operated by member states or by private parties	

Management. – Management's task is to understand the NIS2 requirements and risk management efforts. Management has direct responsibility in the process of identifying and addressing cyber security risks and ensuring compliance with NIS2 requirements

Risk management. – Within the risk management process, the risk is identified, the probability and severity of the risk are taken into account as risk factors and the consequences of potential risks are predicted [17–18]. The NIS2 regulation, similar to NIS, provides discretion to regulated entities in setting their own rules and safeguards when it comes to the security of their systems. This type of regulation is known as "self-regulation" because it allows businesses to regulate themselves, while providing government authorities with the necessary control mechanisms to ensure that the procedures of regulated entities are appropriate and proportionate [19]. Hence the regulation mentioned by the NIS2 Directive can also be treated as a kind of metaregulation. Meta-regulation offers flexibility that is particularly important considering the complexity of information systems and different types of cyber attacks, but on the other hand it introduces certain difficulties when analyzing whether a regulated company fully

complies or does not fully comply with regulatory requirements. The shortcomings of meta-regulation can be overcome by proper oversight of all activities.

Supervision and fines. – Within the framework of the NIS Directive, the competent authorities of the member states had the opportunity to request information from OES about the current state of their information systems and findings from security audits. In addition, the competent authorities based on their own opinion could issue binding orders to those companies in order to strengthen their security protection. This approach assumed that supervisors have the necessary resources and skills to assess these risks. NIS2 increases surveillance as member states are required to establish investigative measures such as: regular audits, security surveillance of targeted system, inspections that can be conducted within the user's data centers or outside them, including random checks and security scans. In addition, for OES, member-countries should dedicate or appoint supervisor who will monitor the companies' compliance with risk management measures. In accordance with Article 30 of the NIS2 Directive, the powers of competent authorities are extended in the domain of supervision of important entities, which are similar in nature to the powers and measures imposed on OES. The main difference in the supervision of OES and important entities is that for the latter no supervisors are appointed to monitor companies' compliance with risk management measures. Perhaps more importantly, in accordance with Article 30 of the NIS2 Directive, important entities are subject to supervision only on the basis of evidence or indications of non-compliance. Such an approach can be an obstacle in the battle to increase the level of cyber security in the EU. High administrative fines provided by the NIS2 Directive can be treated as a bridge that can help to overcome these shortcomings [20]. Namely, the NIS2 Directive foresees relatively high administrative fines for OES (maximum of 10 million euros or up to 2% of the total annual turnover), while the fines for important entities amount to a maximum of 7 million euros or up to 1.4% of the annual turnover of the company. In order to ensure real liability in case of non-compliance, the NIS2 Directive provides provisions for the liability of natural persons in senior management positions in companies covered by the scope of the new NIS2 Directive. It is to be expected that administrative penalties for non-compliance can have a positive effect on companies [20].

Reporting. – When it comes to incident reporting, the right balance needs to be struck between the need for prompt reporting to avoid the potential spread of incidents and the need for detailed reporting that can help us to learn from each incident. NIS2 provides multiple ways of reporting incidents. Affected companies have a deadline of 24 hours from the moment they learn about the incident to give an early warning to the local CSIRT in order to request assistance, guidance or operational advice how to implement possible measures to mitigate the consequences of the incident. An early warning should be followed by a detailed incident report within 72 hours of becoming aware of the incident, while a final report should be submitted a month later.

Business continuity. – Organizations must be well prepared how to ensure business continuity in the event of a major cyber incident. This includes, for example, a recovery system, emergency procedures, the establishment of a crisis response team, and communication protocols in the event of a crisis.

4. HOW COMPANIES SHOULD ADAPT TO THE NIS2 REGULATION

Considering that the deadline for Member States to transpose NIS2 into national law is October 2024, companies subject to regulation by this directive must familiarize themselves with NIS2 recommendations.

Not all requirements defined in the NIS2 Directive apply equally to all businesses and organizations. The requirements of this directive vary depending on the size of the business and the role of that organization in society. In any case, there are a number of requirements that companies must meet in order to comply with the NIS2 Directive.

Asset inventory. – Asset inventory incorporates software tools and processes that enable record keeping of all hardware and software within an enterprise. In essence, it is a platform that will enable the automatic discovery of devices, applications and users, regardless whether they are mobile, static, IoT or in the cloud. Hardware asset management tool can configure and monitor the various relationships of every business-critical asset in company network. This may help during a change in the network infrastructure or during root cause analysis of a problem. Software Asset Management can help in keeping the track of company software assets and

licenses. Asset inventory is a basic prerequisite for building a mature and comprehensive security model, given that in this way all devices can be monitored and analyzed in terms of potential vectors of an attack.

Threat detection. – Threat detection is a process that includes timely identification of potential threats and creation of a response before the threat affect the business. When it comes to a company with multiple locations, an integrated and centralized solution is needed that will cover not only the headquarters but also the remote locations. There are several management systems that enable threat detection, such as SIEM (Security Information and Event Management), SOAR (Security Orchestration, Automation, and Response), XDR (Extended Detection and Response).

SIEM is a solution that aggregates log data from multiple sources into one centralized platform. SIEM allows businesses to identify potential security threats and vulnerabilities before gaps can be exploited.

SOAR is a solution that identifies vulnerabilities based on vast amounts of collected SIEM data. SOAR uses automated workflows that enables mitigation without human intervention. Bearing in mind that SOAR is dependent on SIEM, these systems are often used in conjunction.

XDR is a cyber security solution that uses AI to detect anomalies in users behavior, as well as in the routers, servers, and endpoints of the network. XDR enables the automatic disconnection from a network of end devices that exhibit suspicious activity

Network segmentation. – Network segmentation is a security technique based on dividing a network into smaller, distinct subnets in order to define appropriate security controls at the level of each subnet eliminating a possibility for single point of failure. For example, if there is a cyber security breach in one subnet it will not affect the whole network. Network segmentation is usually done through a combination of firewalls, creation of Virtual Local networks (VLAN) or subnets. Firewalls are deployed inside the network to create internal zones that divide functional areas from one another. A VLAN is a way of logically separating a group of computers into a separate network. This means they will only communicate with each other and not with any other devices connected to the same physical network. Subnets use IP addresses to create a logical partition of an IP network into multiple, smaller network segments.

Policies and procedures for the use of encryption. – Increasing the use of encryption is one of the main goals of NIS2. Of course, a large part of the communication is already encrypted using protocols such as ssh and https when it comes to computer-computer or computer-server communication or by using IPSEC, MPLS VPN or SDWAN type of services when it comes to security connecting one or more remote locations.

Security procedures for data access. – Security procedures for data access should apply not only to employees within the company, but they should also cover the relationship between the company and the direct supplier. There are several types of management systems that can enhance the security procedures for data access. In this paper we will focus on two, maybe the most important systems: PAM (Privileged Access Management) solutions and MFA (Multi-Factor Authentication). PAM is a solution that helps protect organizations against cyber threats by making sure that people have only the necessary levels of access to do their jobs. This solution is exceptionally important when the company collaborates with their supply chain in a digital manner. MFA is a login process that requires users besides the password to enter more information like a code sent to their email, SMS, scanning a fingerprint, or simply answer a secret question.

Business continuity plan. – A plan for managing business operations should be created in a way that will guarantee access to IT systems and their operational functions during and after a security incident. It should consist of at least three steps. As part of the first step, the critical on-premise and cloud infrastructure should be scanned. The second step is prioritizing critical systems, while the third step is introducing regular backups and testing the backups and business continuity process to ensures that data recovery is possible in the event of a real crisis.

Risk management and periodic risk assessments. – Risk assessment is vital for any organization, but risk assessment is not a one-time job. New vulnerabilities in the systems may appear due to changes in network configuration and business processes or due to emerging new threats in the ever-changing cyber security landscape. The risk assessment consists of two basic parts. The first part refers to the Security Review & Gap Analysis whose task is to generate a complete and comprehensive process for defining security risk strategies based upon your objectives, security posture and status. The

second part refers to periodically performing network vulnerability testing. Vulnerability assessment and penetration testing are the most common methods for assessing the security risk of systems [21] (Weber et al., 2017). Many people believe that vulnerability assessment and penetration testing are two same terms, but actually these two terminologies differ to some extent. Vulnerability assessment is defined as the automatic identification of system weaknesses, while penetration testing mainly refers to a form of stress testing that detects weaknesses in networks and sets measures to overcome these vulnerabilities in the network

Incident response and reporting. – The NIS2 Directive demands timely and appropriate reporting, so regulated companies need to know how to respond before an incident occurs: how to collect warning information, how to track incidents, how to report actual incidents and to whom. The threat-detection solution described above should be able to help operations and security teams to easily comply with NIS2 reporting prerequisites.

Cyber security training and a practice for basic computer hygiene. – Given that the majority of successful cyber attacks occur as a result of targeted fishing campaigns, NIS2 requires organizations to provide training to their management and employees to deepen their cyber security knowledge. Within the cyber security framework, various trainings can be included such as: awareness trainings, continuous training program and courses appropriate to the employee level in the organization, type of work, and exposure to security threats.

5. N. MACEDONIA – CYBER SECURITY LEGAL FRAMEWORK, ADOPTION OF NIS2, CHALLENGES AND RECOMMENDATIONS

N. Macedonia is slowly but steadily working towards developing a secure cyber environment. The Government of N. Macedonia aims to improve its ability to protect infrastructure such as energy, telecommunications, and e-services and ensure that systems and structures are in place to meet the future requirements of international allies such as the European Union and NATO. The first significant step was taken in 2018 when the Cyber Security Strategy (2018–2022) including an Action Plan was developed (available at www.mioa.gov.mk). Through the identification of main stakeholders and through the identification of goals, measures, and activities, the strategy and the action plan aim was focused on fostering the development of a safe, secure, reliable and resilient digital environment in the country.

In 2021, N. Macedonia adopted the National ICT strategy (2021–2025) (available at www.mioa.gov.mk). The strategy had six pillars:

- Interoperability and government infrastructure;
- Centralization of ICT and e-government services;
- Improved people digital skills;
- R&D (research & development);
- Data protection;
- Digital services.

In 2021, N. Macedonia signed a memorandum of understanding with NATO which aims to facilitate the exchange of information and best practices when it comes to cyber threats. Ministry of Defense in accordance with the National Cyber Security Strategy, the EU Strategy and NATO standards developed the Strategy for Cyber Defense. This strategy aims to provide improved protection of national interests by developing and strengthening local capabilities to monitor and reduce the impact of cyber security risks.

In addition to the adoption of the National Cyber Security Strategy (2018–2022), a series of other documents relevant to cyber security in the country were adopted. For example, with the adoption of the Law for Electronic Communications, a National Computer Incident Response Center (MKD-CIRT) was established as a separate unit of the Agency for Electronic Communication. MKD-CIRT, similar to the CIRTs in the EU member-states, aims to raise the protection of network and information security to a higher level.

The Law on Personal Data Protection was originally adopted in 2005. As a result of the need to harmonize this law with the EU Regulation regarding the Protection of Personal Data (GDPR), a new Law on Personal Data was adopted in February 2020. From August 24, 2021, the Law on Personal Data is fully in force.

Currently, there are a number of documents related to cyber security that are under development. The Ministry of Defense is working on Law on Critical Infrastructure, while the Ministry of Information Society is working on new National ICT Strategy (2023–2030) and new National Cyber Security Strategy (2023–2030). In parallel Ministry of

Information Society is also working on preparing the Law on Security of Network and information Systems, and Digital Transformation.

The aim of the Law on Critical Infrastructure is to define critical physical infrastructure sectors that must be protected. This law identified 9 (nine) critical sectors:

- Energy (production, including dams, mining, storage, transportation of energy, and energy distribution, etc.).
- Transport (road, rail, air and water traffic).
- Banking systems and infrastructure of the financial markets.
- Health (health care, production, trade and control over medicines).
- Water supply (water supply and drainage systems).
- Food (food production and supply).
- Production, storage and transportation of dangerous substances (chemical, biological, radiological and nuclear materials).
- Public services (ensuring public order and peace, protection and rescue, emergency medical assistance).
- Digital infrastructure, communication and information technologies (electronic communications, data transfer, information devices and installations, audio and audiovisual media services, etc.).

The owners/operators of critical infrastructure are obliged to create and update the security plan or the equivalent document in accordance with the applicable regulations and are obliged to establish an internal crisis management and crisis communication system for all matters important for the operation of the critical infrastructure.

The new National ICT Strategy 2023–2030 is focused to set a clear roadmap for better digitization of society, which directly affects the quality of life of citizens. The strategy is based on 4 basic pillars:

Pillar 1: Gigabit connectivity and ICT infrastructure). – This pillar consists of three strategic objectives: provision of gigabit connectivity to public institutions, development of Government ICT infrastructure and development of National educational ICT infrastructure.

Pillar 2: Developing digital skills. – This pillar covers the implementation of training programs for development of ICT skills.

Pillar 3: Digital management, with enhanced support for digitization of businesses. – Digital governance consists on development of three strategic objectives: e-services, digital identity, and cyber security.

Pillar 4: ICT enablers and digital innovation. – This pillar consists of three strategic objectives: horizontal platform, open data, promotion of innovation and digitization of SMEs (small and medium enterprises).

The new National Cyber Security Strategy (2023–2030) is prepared taking into account ENISA guidelines and tools for the development of national cyber strategies. This strategy lay on 5 pillars:

- Pillar 1: Building clear and robust cyber security governance structure;
- Pillar 2: Security and resilience of networks, information and communication systems;
- Pillar 3: A society resilient to cyber threats;
- Pillar 4: Minimizing the impact of incidents in cyberspace;
- Pillar 5: National and international cooperation.

Within Pillar 1, the establishment of a National Council for Cyber Security and creation of a SPOC (Single Point of Contact) is foreseen in order to ensure efficient cross-border cooperation with the relevant authorities of other countries, EU member states, European Commission, ENISA and NATO. Within the framework of Pillar 1, the creation of a unique and comprehensive legal framework for cyber security management is also envisaged, through the adoption of a new law, in line with the NIS2 Directive (Directive – EU 2022/2555). Within Pillar 2, in accordance with the NIS2 Directive, high and other critical sectors are defined in the way they correspond with operators of essential services (OES) and Important entities from NIS2.

Another significant document in preparation related to cyber security is the Law on Security of Network and Information Systems, and Digital Transformation. This law aims to provide legal framework that will be in accordance with the NIS2 Directive.

Enacting the appropriate legislation is a step in the right direction when it comes to setting a platform for the upliftment of Cyber Security. In that regard, N. Macedonia is on the right path. However, there are a lot of challenges for Government, infrastructure operators and the private sector that needs

to be addressed. Below are some of our recommendations:

Finalization of strategies related to cyber security: Adoption of National ICT Strategy (2023–2030) and National Cyber Security Strategy (2023–2030).

Effective legal framework: Finalizing laws that are currently in the stage of public debate, such as the Law on Security of Network and Information Systems, and Digital Transformation, and Law on Critical Infrastructure.

Harmonized policies: By adopting the National ICT Strategy, National Cyber Security Strategy and series of laws related to cyber security, the government and key institutions should prevent overlapping of legal provisions by clarifying the roles of each of the institutions separately.

NIS2 compliance: The government should prepare recommendations for the entities that will be regulated by NIS2 in terms of recommended management systems for Asset Inventory, Threat Detection, Encryption, Security procedures for data access, etc. in order to better monitor the compliance with NIS2 Directive.

Education: There is a shortage of qualified cyber security personnel due to an outdated education system and teaching methodologies, non-standardized cyber security job descriptions and qualifications, and a significant brain drain to other countries. The government and educational institutions must start working on the production of qualified personnel.

Public awareness campaign: The government in cooperation with the private sector and civil initiatives should invest more in campaigns aimed at raising awareness of the importance of cyber security. In this way, people would be aware of the risks they may face when using the Internet without adequate protection.

Regional cooperation: Considering that the majority of cyber attacks originate outside the Balkan region, the Government should have a more proactive approach in order to have greater cooperation with other countries from the Western Balkans.

International cooperation: The institutions in N. Macedonia should intensify their efforts to participate in cyber security initiatives and projects, as well as the development of regional, European and international partnerships. N. Macedonia as a country does not have the capacity to independently protect itself from cyber attacks, therefore wider coordination and cooperation is essential.

6. CONCLUSION

Digitization is essential for developing a functional, efficient and modern government and society. The Macedonian government is continuously increasing the number of digital services. The rapid adoption of digital technologies exponentially increases the risk of successful cyber attacks. Developing countries such as N. Macedonia are less resistant to cyber attacks especially when these attacks are aimed at critical infrastructure.

Although N. Macedonia has a solid legal system, it needs to be upgraded by adopting the Cyber Security Strategies (ICT Strategy (2023–2030) and National Cyber Security Strategy) and by bringing into force the Law on Critical Infrastructure and the Law on Security of Network and Information Systems, and Law on Digital Transformation.

Different types of cyber attacks show that N. Macedonia should work even more on creation of an effective response to such cyber attacks threats in order better to protect the national security. Therefore, apart from the completion of the previously mentioned legislation, the focus must be placed on education, harmonized policies, public awareness campaign, regional and international cooperation.

REFERENCES

[1] Statista (2024): Overview. Accessed 27.02.2024. https://www.statista.com/topics/4123/internet-of-things-iot-in-europe/#topic

[2] BIRN (2021): Online intimidation: Controlling the Narrative in Western Balkans.

[3] Taddeo, M. (2013): Cyber security and individual rights. striking the right balance. *Philosophy & Technology*, **26** (4), pp. 353–356.

[4] Gordon, L. A., Loeb, M. P., Lucyshyn, W. (2020): Cybersecurity investments in the private sector: The role of Governments. *Georgetown Journal of International Affairs*, pp. 79–88. Accessed May 17, 2021. http://www.jstor.org/stable/43773651.

[5] Michels, J. D., Walden, I. (2020): Beyond "Complacency and Panic": Will the NIS Directive improve the cybersecurity of critical national infrastructure? *European Law Review*, pp. 25–47.

[6] Clark-Ginsberg, A., Slayton, R. (2018): Regulating risks within complex sociotechnical systems: Evidence from critical infrastructure cybersecurity standards. *Science and Public Policy*, **46** (3), pp. 339–346.

[7] *EU Cybersecurity Strategy*, https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391

[8] *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. https://eur-lex.europa.eu/eli/dir/2016/1148/oj

[9] *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). https://eur-lex.europa.eu/eli/dir/2022/2555/oj

[10] *Regulation (EU) 2016/679* of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). https://eur-lex.europa.eu/eli/reg/2016/679/oj

[11] *Regulation (EU) 2022/2065* of the European Parliament and of the Council of 19 October 2022 on a single market for digital services and amending Directive 2000/31/EC (Digital Services Act). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R2065

[12] *Regulation (EU) 2022/868* of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0868

[13] *Regulation (EU) No 910/2014* of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, https://eur-lex.europa.eu/legal-content/EN/TXT/? uri=uriserv%3A OJ.L_.2014.257.01.0073.01.ENG

[14] *Directive (EU) 2015/2366* of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri =celex%3A32015L2366

[15] *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. https://eur-lex.europa.eu/eli/reg/2022/2554/oj

[16] *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). https://eur-lex.europa.eu/eli/reg/2019/881/oj

[17] Gellert, R. (2020): *The risk-based approach to data protection*. Oxford University Press.

[18] Lin, W. C., Saebeler, D. (2019): Risk-based v. compliance-based utility cybersecurity – A false dichotomy? *Energy Law Journal* **40** (2), pp. 243–282.

[19] Parker, C. (2002): *The Open Corporation: Effective Self-regulation and Democracy*. Cambridge University Press.

[20] Voss, W., Gregory and Bouthinon-Dumas, H. (2021): EU general data protection regulation sanctions in theory and in practice. *Santa Clara High Tech. Law Journal* **37** (1), pp. 1–97.

[21] Weber, R; H., Staiger, D. (2017): *Transatlantic Data Protection in Practice*. Springer.