Katerina Buchkovska*

CYBERSECURITY CHALLENGES IN EMERGING DEMOCRACIES: THE CASE OF NORTH MACEDONIA IN THE CONTEXT OF EURO-ATLANTIC INTEGRATION

Abstract

In recent years, cybersecurity has become one of the central issues in international relations, not only as a technical challenge but also as a matter of national security, diplomacy, and democratic stability. Globally, the main challenges include protecting critical infrastructure, preventing state sponsored or other types of cyber attacks, and ensuring resilience against hybrid threats. For small and resource-limited states, these risks are amplified by limited technical capacity, lack of consistent legislation and dependence on external technologies and expertise.

This paper argues that cybersecurity for North Macedonia cannot be understood in purely technical terms. It is closely tied to democratic governance, regional stability, and the country's commitment to become full-fledged EU member country. Addressing these challenges requires a comprehensive approach: raising cyber awareness on national level, investments in cyber security, alignment with EU/NATO cybersecurity legal framework, cooperation with NATO and EU structures and participation in regional initiatives in the Western Balkans. North Macedonia has no alternative but to place cybersecurity at the top of its national agenda — both as a matter of safeguarding its sovereignty and critical infrastructure and as a prerequisite for positioning itself as an active and effective participant in the global digital order.

Keywords: cybersecurity, cyber awareness, cyber threats, North Macedonia

I. INTRODUCTION

In the past decade, countries all over the world have undergone a rapid digital transformation, which has led to a complete reconfiguration of political, economic and social systems. Cybersecurity and digital resilience have become an integral part of national security strategies of the countries. As governments, businesses and citizens are becoming increasingly dependent on the use of digital infrastructure for communication, trade and delivery of public services, the protection of cyberspace is necessary to safeguard democratic processes and to maintain institutional stability. Cybersecurity comprises different policies, technologies, practices and regulatory frameworks designed to protect digital systems, networks, and data from unauthorised access In addition to its technical aspects, cybersecurity also presents a atrategic and political challenge to emerging democracies which are undergoing a complex transition to stable, functionable democratic societies.

Emerging democracies are more vulnerable to cyber attacks due to the fact that in building their cybersecurity posture, they are faced with new regulatory frameworks, limited technical capacity, and often low public trust in state institutions. Unlike developed countries, emerging democracies must at the same time build digital infrastructure and develop legal and institutional

* Katerina Buchkovska, PhD., Assistant Professor, in International Relations and Diplomacy at the Faculty of Law at International Balkan University–Skopje, ORCID 0009-0000-6243-6035, e-mail: katerina.buchkovska@ibu.edu.mk

mechanisms necessary to protect it. This process creates opportunities for innovation and growth but also exposes these societies to increased risks, including cybercrime, cyber espionage, disinformation campaigns, and hybrid threats that combine technological and political interference to undermine democratic institutions.

Cyber attacks and cyber threats are carried out by both state and non-state actors. The establishment of dedicated cyber military units by many countries creates significant risks, as it increases the potential for cyber warfare and large-scale attacks. Since many activities across land, air, sea, and space now depend on digital systems and cyber infrastructure, disruptions in cyberspace can have serious and wide-ranging consequences.[1]

The importance of cybersecurity in emerging democracies extends beyond protecting technical systems; it directly influences democratic legitimacy, political stability, and the functioning of public institutions. Electoral processes, public administration systems, critical infrastructure such as energy and telecommunications, and media increasingly depend on secure digital environments. Cyber incidents targeting these sectors can disrupt governance, weaken state capacity, and erode public trust in democratic processes.

At the same time, emerging democracies must balance the need for robust cybersecurity measures with the protection of fundamental democratic values, including freedom of expression, privacy, and transparency. The growing security driven measures in cyberspace pose a risk to establishing authoritarian practices that would threaten civil liberties, while insufficient protection exposes societies to external risks and instability. Therefore, cybersecurity policies in emerging democracies requires a multi-layered approach that consists of building technical resilience, democratic accountability and governance principles.

In the digital age, cybersecurity has become a central element of national security, governance, and democratic resilience for every country in the world. For emerging democracies such as North Macedonia, cybersecurity is not merely a technical matter—it is a strategic and political challenge that shapes the country's democratic trajectory, institutional trust, and geopolitical stability.

II. WHAT IS CYBERSECURITY?

Cybersecurity can be viewed from different perspectives. On one level, it might be viewed as a technical field**,** an area focused on safeguarding digital systems, networks, and data from unauthorized access, attacks, or damage. However, cyber security is playing a much larger role in the international arena**.** It is not only a matter of technology, but also a sphere of power and competition among states. Being related to states wellbeing and stability, cybersecurity has become a key part of national security, sovereignty, and national interests**.** It is also closely connected to cyber diplomacy**,** which has become a novel important element of many countries' foreign policy strategies. Today, the ability to ensure cybersecurity is seen as both a sign of technological preparedness and a tool of political influence in the global world.

There have been numerous attempts to define cybersecurity, reflecting its evolving and multidimensional nature. There are dozens of definitions of cyberspace but generally "cyber" is a prefix standing for electronic and computer related activities. One of the most relevant definitions is provided by Joseph Nye, who defines it as: "Cybersecurity involves the protection of computer networks and the information they contain, but it also encompasses the management of cyber

[1] Ugbo, Nosakhare, "The Critical Role of Cyberspace Activities in Enhancing Global Security", International Journal of Science Research and Technology Vol. 8, May, 2025 Editions

power in international relations."[2] The US Department of Defence gives the following definition: "Cyberspace is a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[3]

On the other hand, ENISA, the European Union Agency for Cybersecurity, defines cybersecurity as the "ability of network and information systems to resist, at a given level of confidence, accidental events or unlawful actions that compromise authenticity, integrity and confidentiality of stored or transmitted data and related services".[4] If we go further to explore how relevant institutions define cybersecurity, the International Telecommunication Union views cybersecurity as the "collection of tools, policies, security concepts, safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment and organization and user's assets."[5] In general, we may define cybersecurity as protection of digital infrastructure, data and network systems from attacks and malicious activities in combination with an ability to manage cyber risks and prevent cyber attacks that may affect national security, international relations and political stability.

In view of the importance of cybersecurity in the international realm from academic perspective, Myriam Dunn Cavelty asserts that cybersecurity has become a political construct in which threats to information infrastructures are linked to national security, economic stability, and the maintenance of political order."[6] According to the author, cybersecurity has shifted from a purely technical concern to a political and strategic one, where the protection of information systems is directly linked to the preservation of national sovereignty, economic stability, and public trust. This makes cybersecurity a central topic in global security agendas and a decisive factor shaping inter-state relations.[7]

In recent years, cybersecurity has become one of the most critical issues in contemporary international relations, influencing how states view and understand security, exercise power, and conduct diplomacy in the digital age. In an increasingly interconnected world, digital infrastructures are not only essential for communication and economic growth but are also becoming the backbone of national security systems. As such, the vulnerability of these systems exposes states to new forms of threats—ranging from espionage and disinformation to cyber warfare and critical infrastructure sabotage.

From the perspective of power politics, cybersecurity seems to reflect the logic of competition and deterrence similar to that seen in traditional military domains. Joseph Nye introduced the concept of "cyber power," describing it as the ability to use cyberspace to achieve national objectives, either by defending against or executing cyber operations.[8] United States, China, and Russia increasingly consider cyberspace as a competitive arena for impact and power, leading to an ongoing digital arms race. The increasing spread of state sponsored cyberattacks, such as the 2007 attacks on Estonia,[9] the Stuxnet operation against Iran's nuclear program in

---

[2] Nye, Joseph, "Cyberpower", Belfer Center for Science and International Affairs, Harvard Kennedy School, May 2010

[3] "Cyberspace Operations", Joint Publication,United States Department of Defence, (2018). https://www.onlinelibrary.iihl.org/wp-content/uploads/2021/05/2018-JP-3-12-Cyberspace-Operations.pdf

[4] "ENISA Overview of Cybersecurity and Related Terminology", ENISA, September 2017, available at enisa.europa.eu

[5] https://www.itu.int/en/action/cybersecurity/Pages/default.aspx

[6] *Dunn Cavelty, M. (2008). Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*

[7] *Dunn Cavelty, M. (2008). Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*

[8] Nye, Joseph, "Cyberpower", Belfer Center for Science and International Affairs, Harvard Kennedy School, May 2010

[9] Buresh, D. L. (2020) " A Critical Evaluation of the Estonian Cyber Incident", Journal of Advanced Forensic Sciences ISSN NO: 2692-5915

2010,[10] and the 2017 NotPetya malware incident, demonstrates how cyber capabilities have become instruments of geopolitical and global competitiveness. These incidents have shown that cyber operations can have consequences comparable to conventional acts of aggression, thereby expanding the traditional definition of conflict in international relations.

At the same time, cybersecurity is not solely about conflict but also about cooperation and governance. Because cyberspace transcends national borders, no state can secure it alone. This interdependence has prompted multilateral initiatives aimed at establishing norms and confidence-building measures. The United Nations' Group of Governmental Experts (UNGGE) and the Open-Ended Working Group (OEWG) have both sought to define responsible state behavior in cyberspace and promote transparency in cyber policies[11] Similarly the European Union and NATO have integrated cybersecurity into their collective defense and foreign policy system. The EU Cybersecurity Strategy explicitly emphasizes that a secure digital environment is essential for maintaining trust in democratic institutions and ensuring global stability.[12] These developments point out that cybersecurity has become an inseparable part of diplomatic practice and international governance.

In the meantime, the growing role of non-state actors**,** including independent entities such as criminal groups, hackers and individuals that operate outside direct state control, further complicates the landscape of cybersecurity in international relations. Many scholars argue that cyberspace is now a contested domain where state and non-state actors alike seek to shape the rules and standards of digital behavior. This means that cybersecurity is not only a matter of national policy but also of global interest and negotiation. In summary, cybersecurity has become a defining feature of international relations in the 21st century, linking technology, security, and foreign policy in ways that reshape how we see power in the digital era.

III. THE RISE OF HYBRID THREATS IN THE GLOBAL CONTEXT

The global security in the 21st century has been increasingly impacted by the emergence of hybrid threats which are combination of cyberattacks and disinformation campaigns aimed at destabilizing states and manipulating public opinion. Unlike conventional warfare, hybrid threats function below the threshold of open conflict, misusing the vulnerabilities of digital infrastructure. They represent one of the most pressing challenges to democratic governance, international security, and societal resilience in the digital age.

Hybrid threats are combination of conventional and unconventional means of power. They can include cyberattacks on critical infrastructure, coordinated disinformation campaigns on social media, manipulation of elections, economic pressure, and the use of proxy actors to achieve strategic goals. The advancement of digitalization has made cyber operations faster, cheaper, and harder to trace, which enables both state and non-state actors to achieve political or ideological goals without engaging in direct conflict. This blurring of military, informational, and psychological tactics has redefined how conflicts unfold and how security must be understood.

---

[10] Fruhlinger Josh, "Stuxnet Explained: The First Known Cyberweapon", CSO Online, available at https://www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html

[11] "Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security", United Nations, 2021, UN Digital Library available at https://digitallibrary.un.org/record/3934214?v=pdf

[12] "The EU's Cybersecurity Strategy for the Digital Decade" European Commission (2020), available at https://www.cyber-diplomacy-toolbox.com/EU_Cybersecurity_Strategy_for_the_Digital_Decade.html

Globally, hybrid threats are often used by powerful states seeking to expand influence or undermine rival blocs. Russia's interference in Western elections and its information operations during conflicts in Ukraine and Syria [13]have demonstrated how disinformation can shape narratives and weaken adversaries without the need for military engagement. Similarly, China's use of cyber-espionage and digital propaganda illustrates how technology can be deployed for strategic advantage, from intellectual property theft to the promotion of alternative governance models. These hybrid tactics exploit the openness of democratic systems—free media, pluralism, and digital interconnectivity—to create confusion, polarize societies, and erode trust in institutions.

Cyber attacks are a central component of hybrid strategies. Critical sectors such as telecommunication, energy, transportation and healthcare have become targets of ransom ware and data breaches that disrupt daily life and damage economic stability. The 2017 WannaCry and NotPetya attacks,[14] for instance, demonstrated how malicious software could paralyze entire networks across borders within hours. Such operations are not isolated technical incidents—they are tools of geopolitical competition aimed at weakening the resilience and credibility of states.

Parallel to cyber operations, disinformation campaigns use social media platforms to manipulate public perception. Through bots, fake accounts, and coordinated content, malicious actors amplify divisive narratives, spread conspiracy theories, and delegitimize governments or international organizations.

The global nature of hybrid threats demands multilateral cooperation. NATO, the European Union, and the United Nations have increasingly recognized the hybrid domain as a critical security frontier. Strategies now emphasize the integration of cyber defense, strategic communication, and societal resilience. However, building effective responses requires not only technological capabilities but also public education, media literacy, and democratic safeguards that prevent the misuse of countermeasures for censorship or surveillance.

Hybrid threats represent the new face of power in international relations—subtle, persistent, and multidimensional. By combining cyberattacks, disinformation, and political manipulation, they exploit the very features that define open societies. Addressing them requires a holistic approach that combines security, diplomacy, and democratic integrity to protect both national sovereignty and the global digital order.

In the era of hybrid threats and increasing digital interdependence, critical infrastructure protection has become one of the most important aspects of national and international security. Critical infrastructures particularly in the fields of energy, finance, and telecommunications form the backbone of modern societies and economies. Their disruption, whether by cyberattacks, technical failure, or malicious interference, can have devastating consequences for public safety, economic stability, and everyday life of citizens. As hybrid threats are increasingly targeting these vital systems, ensuring their resilience has become both a strategic priority and a test of state capacity.

The energy sector is one of the most vulnerable areas. Modern energy networks, from power grids to oil and gas supply chains are deeply digitized and connected across borders. This connectivity, while efficient, also creates multiple points of vulnerability. Cyberattacks on energy infrastructure can lead to blackouts, risk industrial production, and create spilling effects across

[13] Giles Keir, "Russian Cyber and Information Warfare Practice", Chatam House, available at: https://www.chathamhouse.org/2023/12/russian-cyber-and-information-warfare-practice

[14] "Notpetya and Wannacry Call for a Joint Response from International Community", The NATO Cyber Defence Center of Excellence, available at https://ccdcoe.org/news/2017/notpetya-and-wannacry-call-for-a-joint-response-from-international-Cooperative community/

other sectors. The 2015 and 2016 cyber attacks on Ukraine's power grid[15] demonstrated the how these attacks may cause real world harm and serve as instruments of political pressure. The 2015 attack disrupted power supply to 230 000 citizens through the implemented SCADA systems while the 2016 attack compromised the industrial production through specialized malware. Similarly, ransomware incidents such as the Colonial Pipeline attack[16] in 2021 demonstrated how vulnerable the critical energy system might be and how eventual attack may generate economic disruption and reveal that nations are not prepared sufficiently to respond to such attacks. In response, many developed countries and international organizations, including NATO and the EU, have prioritized energy cybersecurity through joint frameworks and rapid response teams.

The financial sector is another important target of possible hybrid attacks due to its importance in the state system and its dependence on digital systems. Cyberattacks on banks, payment systems, and financial data can undermine public trust, destabilize markets, and have cross border implications. The 2016 Bangladesh Bank heist,[17] carried out through the SWIFT international payment system, issued false transfer requests totaling nearly $1 billion, successfully stealing $81 million before detection. This attack demonstrated how cybercriminal and potentially state actors can abuse digital systems for both economic gain and strategic influence. Financial systems are not only attractive for theft but also for sabotage and disinformation campaigns that erode trust in monetary institutions. Consequently, the protection of financial infrastructure now requires a combination of technological innovation, strict regulatory frameworks, and international coordination. The EU's Digital Operational Resilience Act (DORA)[18] and the Basel Committee's cyber-resilience principles [19]are examples of EU efforts to strengthen digital systems in finance sector.

Equally critical is the telecommunications sector, which consists of mobile network operators, satellite systems, broadband providers, IoT and network infrastructure. Telecommunication infrastructure has become prime target for cyberattacks. Disrupting communications can paralyze emergency services, disconnect government networks, and provoke information warfare. The spread of misinformation through social media platforms has shown that communication infrastructures are not only technical systems but also psychological and political battlegrounds. Therefore, ensuring their protection involves both technological defense through network monitoring, encryption, and redundancy but also normative defense, such as promoting media literacy and countering hostile information campaigns.

Protecting critical infrastructure requires a multilayered approach that combines technical resilience, international cooperation, and political will. Governments must collaborate with private sector operators, who often own and manage these systems, to develop shared security standards and crisis protocols. On an international level, organizations such as NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE) and the EU Agency for Cybersecurity (ENISA) play essential roles in developing resilience strategies and sharing best practices.

IV. CASE STUDY: NORTH MACEDONIA

[15] "2015 Ukraine Electric Power Attack", MITTRE ATT&CK available at https://attack.mitre.org/campaigns/C0034/

[16] Newsburger, Ema "Ransomware attack forces shutdown of largest fuel pipeline in the U.S", CNBC available at https://www.cnbc.com/2021/05/08/colonial-pipeline-shuts-pipeline-operations-after-cyberattack.html?msockid=36aac200709c677a118cd70b749c6974

[17] Sami A Kabir,Mogammad, "Lessons Learned from the Bangladesh Bank Heist", ISACA, published December 6, 2023, available at https://www.isaca.org/resources/isaca-journal/issues/2023/volume-6/lessons-learned-from-the-bangladesh-bank-heist

[18] DORA Regulation, EU official site available at https://www.regulation-dora.eu

[19] "Cyber Resilience, Range of Practices", Basel Committee on Banking Supervision, December 2018 available at https://www.bis.org/bcbs/publ/d454.pdf

North Macedonia occupies a strategically significant position in the Western Balkans. The country became a full fledged member of the North Atlantic Treaty Organization (NATO) on 27 March 2020, which was a historic step in its Euro Atlantic integration path. This accession represented not only a major security guarantee but also a strong affirmation of North Macedonia's Euro-Atlantic orientation. Membership in NATO placed the country within the collective defense framework of the Alliance, strengthening regional stability in the Western Balkans and consolidating its role as a contributor to international peacekeeping missions. According to NATO's official statements, North Macedonia's accession presents an additional guarantee to the security architecture of Southeastern Europe by closing the last gap in the alliance's coverage across the Balkans.[20]

Parallel to its NATO integration, North Macedonia has continued to pursue full membership in the European Union, maintaining the status of an official EU candidate country since 2005. The country's EU accession process has been marked by significant political and diplomatic challenges, most notably the 30 years long-standing name dispute with Greece, which was resolved through the Prespa Agreement in 2018. With the agreement, the country changed its constitutional name to the Republic of North Macedonia which led to unblocking both NATO accession and the opening of EU accession negotiations. Although North Macedonia has made progress in areas such as democratic governance, judicial reform, and regional cooperation, the accession process has been delayed due to bilateral disputes and shifting political priorities within the EU[21]. Nonetheless, the country remains firmly aligned with the EU's Common Foreign and Security Policy (CFSP), including its positions on sanctions, cyber resilience, and digital governance.

The integration of North Macedonia within the Euro-Atlantic structures requires a high level of cybersecurity preparedness, as digital infrastructure could be ill-used not only by criminal groups but also by state and non-state actors usually aiming at undermining democratic institutions and influencing political processes.

Cybersecurity challenges in emerging democracies often manifest through disinformation campaigns, election interference, and attacks on critical infrastructure. North Macedonia, like several other countries in the region, has faced waves of false news and cyber propaganda, particularly around key political moments such as elections or sensitive policy debates about EU integration, regional cooperation, or relations with neighboring states.[22] These campaigns often exploit existing political polarization and public distrust, aiming to weaken democratic institutions and reduce citizen confidence in the political process. For instance, misinformation on social media platforms can shape public perception and erode trust in democracy and democratic governance. Ahead of the 2018 referendum, the country was targeted by disinformation activities aiming to influence public opinion to boycott the referendum. These campaigns involved national and international actors and highlighted the country's vulnerability to information manipulation.[23]Between March 2022 and February 2023 a study found more than 4,000 articles

[20] "North Macedonia joins NATO as 30th Ally", NATO Official Newsroom available at https://www.act.nato.int/article/north-macedonia-joins-nato-as-30th-ally/

[21] EU Commission, North Macedonia Report available at https://enlargement.ec.europa.eu/system/files/2023-11/SWD_2023_693%20North%20Macedonia%20report.pdf

[22] "Russian FIMI in North Macedonia: Exploiting Vulnerabilities Through Bilateral Disputes", Case Study, Institute for Communication Studies and Respublika, available at https://respublica.edu.mk/wp-content/uploads/2025/11/russian-fimi-in-n-macedonia_eng.pdf

[23] Pankovski Marko, Rechica Vlora, "Countering Disinformation in Macedonia: How can Parliament Rise to the Occasion?", Center for European Security Studies, CESS Policy Brief No. 6, February 2022

and 10,000 Facebook posts in North Macedonia tied to pro-Russian influence operations. These used Russian state-controlled media content and coordinated dissemination on Facebook, trying to shift public sentiment.[24]

Institutional capacity also remains a challenge. While North Macedonia has made significant progress in establishing legal frameworks and national cybersecurity strategies, it still faces a shortage of skilled professionals, limited coordination between public institutions, and gaps in public awareness. This makes the state administration more vulnerable to phishing, ransomware and other cyberattacks targeting ministries, municipalities, and public services. Moreover, as public services and elections increasingly rely on digital systems, ensuring their integrity and resilience becomes essential for maintaining democratic legitimacy.

North Macedonia has been facing a growing number of cyberattacks targeting critical sectors such as energy, finance, water supply, and healthcare. High-profile incidents, including the Health Insurance Fund attack in 2023[25], and the MEPSO attack[26], have caused significant disruptions to public services, exposing how vulnerable these sectors were. The attack on the State Election Commission during election time, just before the final results were announced, caused a stir and led to voter distrust regarding the credibility of the results.[27]

These incidents illustrate how both cyber attacks and disinformation have become tools in hybrid threats in North Macedonia. The cyber attacks target public institutions and critical infrastructure, while disinformation campaigns focus on policy issues such as elections, referenda and societal cohesion. The merging of these raises risks for national security, democratic governance and public trust in institutions.

V. CURRENT DIGITAL LANDSCAPE

North Macedonia made a significant step towards in cybersecurity in 2025 by adopting the Law on the Security of Networks and Information Systems,[28] fully aligned with the European Union's NIS 2 Directive. This law, published in the Official Gazette in July 2025, establishes for the first time a comprehensive legal framework for cybersecurity in the country, harmonizing national legislation with EU standards and introducing obligations for public institutions and critical sectors to improve cyber risk management and incident response.

Although the law was scheduled to enter into force on January 1 2026, the preparation and adoption of necessary by-laws and regulations has delayed full implementation. At present, secondary legislation is being drafted, in particular rules on critical infrastructure protection and cybersecurity workforce development, which are essential for the law's operational effectiveness.

[24] "Presentation of Study on Russian Propaganda, Influence and Disinformation in North Macedonia", available at https://new.mia.mk/en/story/presentation-of-study-on-russian-propaganda-influence-and-disinformation-in-north-macedonia

[25] "Хакерски напад врз Фондот за здравство, не се исплаќаат боледувања и не се отвараат породилни", available at https://telma.com.mk/2023/02/08/hakerski-napad-vrz-fondot-za-zdravstvo-ne-se-isplakjaat-boleduvanja-i-ne-se-otvaraat-porodilni/, published 08.02.2023

[26] "MEPSO is Facing a Cyberattck, the Network and Power Supply are not Threatened", Sloboden Pecat, available at https://www.slobodenpecat.mk/en/mepso-se-soochuva-so-kibernapad-ne-se-zagrozeni-mrezhata-i-snabduvanjeto-so-struja/

[27] Stojkovski Bojan, "North Macedonia Election Commission "Cyber- Attacked During Polls", Balkan Insight, July 16, 2020 available at https://balkaninsight.com/2020/07/16/north-macedonia-election-commission-cyber-attacked-during-polls/

[28] Закон за безбедност на мрежи и информациски системи 2025, https://mkd-cirt.mk/download/zakon-za-bezbednost-na-mrezi-i-informaciski-sistemi-2025/

In parallel, the government adopted the National Cybersecurity Strategy 2025–2028,[29] setting out the long-term vision and priorities for building a secure, resilient, and trusted digital environment for citizens, institutions, and the economy. This strategy identifies key areas such as risk mitigation, protection of digital infrastructure, human capacity building, and international cooperation as foundational elements of the country's cybersecurity ecosystem.

Together, the new law and the strategic policy framework mark a major step in North Macedonia's efforts to protect its digital systems, align with EU standards, and respond more effectively to potential cyber attacks on central and local government level, the Parliament, the courts, independent state bodies and regulators but also the medium and large private companies from critical infrastructure sectors. The new law defines all entities in the so called high risk sector by their importance and relevance to national security.

According to the provisions of the new law, the primary authority responsible for cybersecurity across central and local executive institutions is the Ministry of Digital Transformation (GOV-CIRT). The National Cyber Incident Response Centre (MKD-CIRT) within the Agency for Electronic Communication will be responsible for other entities (regulators, Parliament, courts, private sector entities, etc.). The Ministry will act as a national single point of contact with EU institutions responsible for cybersecurity such as European Commission, ENISA, EU-CyCLONe but also NATO and other relevant institutions and agencies, enabling timely information exchange, coordination and cross-border cooperation.

The law foresees activities to raise public awareness of cybersecurity and organize training for public administration. The goal is to build a culture of "cyber hygiene" and institutional resilience. The law foresees management of potential cyber risks and implementing preventive and protective measures, mandatory reporting of incidents and threats by relevant institutions and professional support from the competent authorities at the request of the affected entities.

VI. NORTH MACEDONIA: CYBERSECURITY AND THE EU INTEGRATION

Cybersecurity is becoming one of the most important benchmarks for Western Balkan countries within their EU accession framework. It is no longer viewed only in technical terms, but in a much broader dimension, encompassing national security, information-sharing strategies, and digital stability. For North Macedonia, as a candidate country, compliance with the EU digital acquis represents both a regulatory and political requirement. In this context, digital requirements include network security, data protection, and the resilience of critical infrastructure. Furthermore, in the EU negotiation process and the alignment of domestic legislation with EU standards, cybersecurity is closely linked to clusters related to the internal market, digital transformation, and the rule of law. The state's capacity to respond to cybersecurity needs is, in a way, a litmus test of its overall institutional capacity. It shows the level od preparadness of the state apparatus to respond to different threats, crisis and the ability for coordination. It is also necessary to reach compliance in both public and private sector. Any disfunctionalities in the phases of cybersecurity implementation may lead to profound institutional weaknesses which will eventually slow the pace of integration.[30]

[29] Стратегија за сајбер безбедност 2025-2028, Министерство за дигитална трансформација, https://mioa.gov.mk/mk-MK/news/strategija-za-sajber-bezbednost-2025-2028.nspx

[30] European Commission, Progress Report on North Macedonia (2024),available at https://nkeu.mk/en/2025/06/05/european-commission-report-on-north-macedonia-for-2024/

In terms of the Rule of Law, there is a strong connection between state capacity and cybersecurity related issues. Although this dimension is not often sufficiently emphasized, cybersecurity has become an increasingly important aspect of the EU integration process. The European Union is placing growing importance on building cyber-resilient models of governance capable of protecting electoral processes, digital infrastructure and platforms, as well as preventing foreign interference. In emerging democracies, cyber risks might seriously affect the integrity of democratic processes. Weak institutional mechanisms, the absence of effective incident response teams, unclear lines of responsibility during cyberattacks, and insufficient monitoring of digital systems may significantly reduce public trust and undermine democratic governance. As a result, cybersecurity becomes an inseparable part of the EU`s broader conditionality mechanisms, linking tehnical capacity with democratic standards.[31]

The digital infractruture system of one country like in it or not has its own cons besides the pros. North Macedonia, like many other Balkan countries, relies heavily on external technologies, platforms, software solutions and expertise on digital domain. It means that its digital sovereignity is constantly disrupted and these dependencies could be exploted during geopolitical tensions.

As the EU strongly advocates the concept of digital sovereignty while at the same time requiring candidate countries to comply with EU standards on cybersecurity and digitalization, this creates a real dilemma for North Macedonia regarding the choice of providers for digital infrastructure, software, and platforms. It also raises important questions concerning the security and storage of data, as well as alignment with EU certification protocols and standards. If a candidate country lacks the capacity to adequately address these issues, this may create greater risks and vulnerabilities within its own digital system, while also posing challenges and potential risks to the EU Digital Single Market.[32]

In building the digital resilience of a country, media literacy and public trust play a crucial role. One of the most disintegrative factors in a democratic society is the influence of disinformation campaigns. Their impact is not only the result of weak response capacities within the system, but also of low levels of digital literacy and limited public trust in the media and institutions.

Therefore, the EU is placing increasing emphasis on information integrity, a concept that encompasses regulatory policies, laws and bylaws, as well as education in digital literacy across all levels of society. For North Macedonia to keep pace with strengthening societal resilience, the country needs to integrate cybersecurity into education policies, media regulation frameworks, and civil society engagement. Without addressing these dimensions, technical and legal reforms risk remaining insufficient in effectively countering hybrid threats.[33]

In this direction, it is equally important to promote a strong cybersecurity culture in order to raise public awareness and improve understanding of cyber threats, while also building and advancing the necessary institutional and professional capacities for protection. To achieve this goal, it is essential for the government to focus on the development of comprehensive cybersecurity awareness programs targeting the general population, businesses, and educational institutions, with the aim of improving understanding of cyber threats, promoting safe online practices, and emphasizing the importance of incident reporting. In addition, following the EU

[31] European External Architecture, Strategic Communication and Disinformation in Western Balkans (2022), https://www.eeas.europa.eu/eeas/eeas-strategic-communication-task-forces_en

[32] Threat Landscape Report 2023, ENISA, available at https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf

[33] Code of Conduct on Disinformation, European Commission, available at https://digital-strategy.ec.europa.eu/en/library/code-conduct-disinformation

reccomendations, it is very important to take concrete steps toward integrating cybersecurity education and training into the formal education system, with a particular focus on developing the skills and knowledge necessary for building a cyber-resilient workforce.[34]

In order to build a comprehensive approach toward cybersecurity and create cyber resilience, North Macedonia is working on several strategic priorities. One of the key objectives is the development of a cyber-resilient ICT infrastructure and the identification and implementation of adequate solutions for the protection of national interests and critical systems. In the context of accession to the European Union, North Macedonia is required to progressively align its national legislation and institutional framework with EU cybersecurity standards, particularly those related to risk management, protection of critical infrastructure, and incident response mechanisms under the NIS2 Directive framework. This compliance is part of the EU's broader approach to building a secure Digital Single Market, where resilience of ICT systems is essential for economic stability, cross-border data flows, and trust in digital services. Strengthening cyber-resilient infrastructure therefore serves both a national security function and a compliance function within the EU integration process, ensuring compatibility with European standards for digital governance and critical infrastructure protection.[35]

Another important priority is the strengthening of national capacities for prevention, research, and effective response to cybercrime, as well as enhancing cyber defence capabilities aimed at protecting national interests and reducing existing and potential risks in cyberspace. The signing of the Security and Defence Partnership between the EU and North Macedonia on 19 November 2025, aimed at establishing a political framework to strengthen dialogue and cooperation on security and defence matters, represents an important step also in the field of cybersecurity cooperation. Although the agreement is framed in broader security and defence terms and is not exclusively focused on cyber issues, it provides a foundation for further strengthening alignment with EU security standards, including in the area of cybersecurity and digital resilience.[36]

In parallel, greater emphasis must be placed on cooperation and information exchange at both the national and international levels, particularly between state institutions, critical infrastructure operators, private sector entities, and international partners. Such coordination is essential for improving cyber resilience, incident response, and the overall security of the digital environment.[37]

VII. CONCLUSION

Cybersecurity is an important element on the Euro-Atlantic path of North Macedonia. Meeting EU and NATO standards demands not only legal alignment but also development of a functional institutional system capable of responding to emerging cyber threats and cyber attacks. Joint cooperation and coordination among state institutions is crucial, particularly the distribution

[34] Reccomendations to Address Key Cybersecuriy Challenges in North Macedonia, Impetus Center for Internet Development and Good Governance, available at: https://impetus.mk/wp-content/uploads/2024/10/recommendations-to-address-key-cybersecurity-challenges-in-north-macedonia-.pdf

[35] EU Cybersecurity Act, European Commission, available at: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

[36] New Security and Defence Partnership Between EU and North Macedonia to Strengthen Capabilities and Cooperation, European Interest, available at:https://www.europeaninterest.eu/new-security-and-defence-partnership-between-the-eu-and-north-macedonia-to-strengthen-capabilities-and-cooperation/

[37] National Cybersecurity Strategy in Western Balkan Economies, The Geneva Centre for Security Sector Governance, available at: https://www.dcaf.ch/national-cybersecurity-strategies-western-balkan-economies

of responsibilities between ministries, agencies, and regulatory bodies in countering cyber attacks. Better coordination enables more effective information exchange, quicker decision-making, and stronger accountability during cyber incidents.

Apart from regulatory and institutional reforms, investment in human workforce capacity is equally important. Strengthening cybersecurity education, expanding digital skills, and providing continuous professional training for public officials and private sector professionals can significantly improve national resilience. Empowering citizens to recognize disinformation protect their data, and act responsibly online strengthens both national security and public trust in democratic institutions.

Another key dimension is the promotion of public private partnerships for cyber defense. As critical infrastructure such as energy, finance, health, and communications is largely managed by private entities, effective collaboration between the public and private sectors is more than necessary. These partnerships can enhance early warning systems, facilitate knowledge sharing, and foster joint incident-response mechanisms.

Regional cooperation within the Western Balkans presents important component in cybersecurity development. Given that cyber attacks are not traceable and transcend borders, cooperation through shared practices, compatible legislation, and coordinated responses contributes to greater regional stability and aligns national efforts with wider European security frameworks.

In this context, North Macedonia will have to adapt to the rapid digital transformation and strengthen experience sharing process with its neighbors. As a NATO member and EU candidate country, the country's progress demonstrates that cybersecurity policy is not only a technical requirement but also an integral part of institutional development, democratic stability, and successful European integration.

Bibliography

1. Ugbo, Nosakhare, "The Critical Role of Cyberspace Activities in Enhancing Global Security", International Journal of Science Research and Technology Vol. 8, May, 2025 Editions
2. Nye, Joseph, "Cyberpower", Belfer Center for Science and International Affairs, Harvard Kennedy School, May 2010
3. "Cyberspace Operations", Joint Publication ,United States Department of Defence, (2018). https://www.onlinelibrary.iihl.org/wp-content/uploads/2021/05/2018-JP-3-12-Cyberspace-Operations.pdf
4. "ENISA Overview of Cybersecurity and Related Terminology", ENISA, September 2017, available at enisa.europa.eu
5. https://www.itu.int/en/action/cybersecurity/Pages/default.aspx
6. Dunn Cavelty, M. (2008). Cyber-Security and Threat Politics: US Efforts to Secure the Information Age
7. Buresh, D. L. (2020) " A Critical Evaluation of the Estonian Cyber Incident", Journal of Advanced Forensic Sciences ISSN NO: 2692-5915
8. Fruhlinger Josh, "Stuxnet Explained: The First Known Cyberweapon", CSO Online, available at https://www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html
9. Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security", United Nations, 2021, UN Digital Library available at https://digitallibrary.un.org/record/3934214?v=pdf

10. “The EU’s Cybersecurity Strategy for the Digital Decade” European Commission (2020), available at https://www.cyber-diplomacy-toolbox.com/EU_Cybersecurity_Strategy_for_the_Digital_Decade.html
11. Giles Keir, “Russian Cyber and Information Warfare Practice”, Chatam House, available at: https://www.chathamhouse.org/2023/12/russian-cyber-and-information-warfare-practice
12. “Notpetya and Wannacry Call for a Joint Response from International Community”, The NATO Cyber Defence Center of Excellence, available at https://ccdcoe.org/news/2017/notpetya-and-wannacry-call-for-a-joint-response-from-international-Cooperative community
13. “2015 Ukraine Electric Power Attack”, MITTRE ATT&CK available at https://attack.mitre.org/campaigns/C0034/
14. Newsburger, Ema “Ransomware attack forces shutdown of largest fuel pipeline in the U.S”, CNBC available at https://www.cnbc.com/2021/05/08/colonial-pipeline-shuts-pipeline-operations-after-cyberattack.html?msockid=36aac200709c677a118cd70b749c6974
15. Sami A Kabir,Mogammad, “Lessons Learned from the Bangladesh Bank Heist”, ISACA, published December 6, 2023, available at https://www.isaca.org/resources/isaca-journal/issues/2023/volume-6/lessons-learned-from-the-bangladesh-bank-heist
16. DORA Regulation, EU official site available at https://www.regulation-dora.eu
17. “Cyber Resilience, Range of Practices”, Basel Committee on Banking Supervision, December 2018 available at https://www.bis.org/bcbs/publ/d454.pdf
18. North Macedonia joins NATO as 30th Ally”, NATO Official Newsroom available at https://www.act.nato.int/article/north-macedonia-joins-nato-as-30th-ally/
19. EU Commission, North Macedonia Report available at https://enlargement.ec.europa.eu/system/files/2023-11/SWD_2023_693%20North%20Macedonia%20report.pdf
20. “Russian FIMI in North Macedonia: Exploiting Vulnerabilities Through Bilateral Disputes”, Case Study, Institute for Communication Studies and Respublika, available at https://respublica.edu.mk/wp-content/uploads/2025/11/russian-fimi-in-n-macedonia_eng.pdf
21. Pankovski Marko, Rechica Vlora, “Countering Disinformation in Macedonia: How can Parliament Rise to the Occasion?”, Center for European Security Studies, CESS Policy Brief No. 6, February 2022
22. “Presentation of Study on Russian Propaganda, Influence and Disinformation in North Macedonia”, available at https://new.mia.mk/en/story/presentation-of-study-on-russian-propaganda-influence-and-disinformation-in-north-macedonia
23. “Хакерски напад врз Фондот за здравство, не се исплаќаат боледувања и не се отвараат породилни”, available at https://telma.com.mk/2023/02/08/hakerski-napad-vrz-fondot-za-zdravstvo-ne-se-isplakjaat-boleduvanja-i-ne-se-otvaraat-porodilni/, published 08.02.2023
24. “MEPSO is Facing a Cyberattck, the Network and Power Supply are not Threatened”, Sloboden Pecat, available at https://www.slobodenpecat.mk/en/mepso-se-soochuva-so-kibernapad-ne-se-zagrozeni-mrezhata-i-snabduvanjeto-so-struja/
25. Stojkovski Bojan, “North Macedonia Election Commission “Cyber- Attacked During Polls”, Balkan Insight, July 16, 2020 available at https://balkaninsight.com/2020/07/16/north-macedonia-election-commission-cyber-attacked-during-polls
26. Закон за безбедност на мрежи и информациски системи 2025, https://mkd-cirt.mk/download/zakon-za-bezbednost-na-mrezi-i-informaciski-sistemi-2025/
27. Стратегија за сајбер безбедност 2025-2028, Министерство за дигитална трансформација, https://mioa.gov.mk/mk-MK/news/strategija-za-sajber-bezbednost-2025-2028.nspx
28. European Commission, Progress Report on North Macedonia (2024),available at https://nkeu.mk/en/2025/06/05/european-commission-report-on-north-macedonia-for-2024/
29. European External Architecture, Strategic Communication and Disinformation in Western Balkans (2022), https://www.eeas.europa.eu/eeas/eeas-strategic-communication-task-forces_en

30. Threat Landscape Report 2023, ENISA, available at: https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf
31. Code of Conduct on Disinformation, European Commission, available at https://digital-strategy.ec.europa.eu/en/library/code-conduct-disinformation
32. Reccomendations to Address Key Cybersecuriy Challenges in North Macedonia, Impetus Center for Internet Development and Good Governance, available at: https://impetus.mk/wp-content/uploads/2024/10/recommendations-to-address-key-cybersecurity-challenges-in-north-macedonia-.pdf
33. EU Cybersecurity Act, European Commission, available at: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act
34. New Security and Defence Partnership Between EU and North Macedonia to Strengthen Capabilities and Cooperation, European Interest, available at:https://www.europeaninterest.eu/new-security-and-defence-partnership-between-the-eu-and-north-macedonia-to-strengthen-capabilities-and-cooperation/
35. National Cybersecurity Strategy in Western Balkan Economies, The Geneva Centre for Security Sector Governance, available at: https://www.dcaf.ch/national-cybersecurity-strategies-western-balkan-economies