CSupMNE
Straightening Up Cybersecurity Posture of Montenegrin Higher Education system

Co-funded by the Erasmus+ Programme of the European Union

issue# 2, August 2025

newsletter

WORD OF THE EDITOR

I am pleased to present the second edition of the CSupMNE Newsletter, marking our ongoing commitment to bolster cybersecurity capacity in the higher education and public sectors of Montenegro.

We first look at the new Information Security Law in Montenegro and how it aligns with the NIS2 Directive from the EU. Then an article covers the ENISA Cyber Stress Test Handbook, and describes a strategic approach to assess the cyber resilience of the institution, allowing for foresight and a method for assessment rather than just assessment. CSupMNE participated in Media Day 2025 with coverage of challenges and forward movement in cybersecurity in Montenegro's private higher education sector. The MontEDIH initiative continues to demonstrate how a strong science-business partnership can build sustainable digital capabilities. Lastly, we reflect on training at AGH University of Kraków, and the sharing of Polish expertise about the implementation of CERT/CSIRT development and SOC for our partners in Montenegro.

I also want to take the opportunity to thank all our project partners, whose contributions, knowledge, and expertise have shaped this issue of the CSupMNE Newsletter.

Prof. Jerzy Duda
AGH University of Kraków

Contents:

Subscribe for CSupMNE newsletters:
https://csupmne.me/newsletters.php

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

What NIS2 Means for Montenegro: Unpacking the New Information Security Law

Andreja Mihailović, PhD
University of Montenegro

Underscoring the unprecedented scope and impact of cyber threats in the digital age, the estimated annual global cost of cybercrime has reached $10.5 trillion in 2025, a startling increase from $3 trillion in 2015 (WEF, 2025). The Western Balkan region is highly vulnerable to cyber-attacks, including state-sponsored hacks on government systems and financially motivated ransomware campaigns, caused by factors such as low cybersecurity awareness, underinvestment in protective measures, and fragmented laws. These systemic weaknesses are routinely exploited by organized cybercriminal networks, who benefit from the borderless nature of cyberspace, operating with relative impunity. According to a 2024 regional risk assessment, traditional policing in South-Eastern Europe is often "ill-equipped to combat cyber threats" (Global Initiative Against Transnational Organized Crime, 2024). Furthermore, inconsistent cross-border cooperation enables cybercriminals to exploit jurisdictional loopholes. Disparities in legal jurisdictions, the complexity and evolving nature of cybercrime, and inadequate enforcement mechanisms continue to challenge the effectiveness of international legal responses (Hasan, 2024).

The European Union Agency for Cybersecurity (ENISA) reports that the current threat landscape is dominated by a handful of persistent and evolving attack types. Ransomware remains the prime threat in Europe, accounting for an estimated 34% of cybersecurity incidents. In its annual threat assessment, ENISA notes that *"DDoS and ransomware rank the highest among the prime threats, with social engineering, data-related threats, information manipulation, supply chain attacks, and malware following"* (ENISA, 2023). In other words, cyber-attacks are growing in both quantity and sophistication – and they target not only data confidentiality but also service availability and public trust. Notably, ENISA observed that the public administration sector was the most targeted in Europe over the past year (~19% of reported incidents), which is consistent with what Montenegro experienced in August 2022.

For Montenegro, the 2022 attack on government infrastructure was a wake-up call: over 150 workstations in 10 ministries were infected with a novel ransomware (dubbed "Zerodate"), websites were knocked offline, and sensitive data was reportedly exfiltrated. The incident, which prompted Montenegro to seek help from FBI cyber teams and NATO allies, highlighted both the country's exposure to cybercriminal gangs and the geopolitical dimension of cyber threats. This was not an isolated case; Montenegro had faced earlier attacks around its 2016 elections and NATO accession in 2017 (Reuters, 2022). In parallel, cybercrime continues to impose a significant and persistent burden on both businesses and individual citizens, manifesting through activities such as online banking fraud, identity theft, and the proliferation of malware on personal devices.

However, international cooperation is strengthening to combat cybercrime: Montenegro is a party to the *Budapest Convention on Cybercrime*, enabling collaboration with European law enforcement on cross-border cyber investigations (Council of Europe, 2001). Additionally, regional initiatives such as the establishment of a new Regional Cyber Capacity Center, supported by France and Slovenia, aim to strengthen cyber capabilities across the Western Balkans (WB3C, 2025). Montenegro further advanced its digital integration by joining the EU's Digital Europe Programme in June 2023, gaining access to funding and collaborative projects in areas such as cybersecurity, artificial intelligence, and advanced digital technologies (European Commission, 2023). This alignment with the broader European digital single market also entails adopting key legislative instruments - Digital Services Act (DSA) and the Digital Markets Act (DMA), reflecting a shared understanding that cyber threats transcend national borders and that Montenegro's resilience will be strengthened through collective action and international cooperation.

The New Information Security Law: Aligning with EU Standards

As a NATO member and EU candidate, Montenegro has ambitiously aimed to meet EU membership criteria by 2028, making the harmonization of its cybersecurity legislation with European standards a strategic priority. In response, the 2024 Law on Information Security marks a significant legislative

advancement, introducing a comprehensive set of obligations designed to align Montenegro's national cybersecurity framework with the European Union's NIS2 Directive and international best practices. The law defines binding responsibilities for public institutions, private sector actors, and operators of critical infrastructure. These obligations mark a significant shift toward a proactive, risk-based model of cyber governance.

Operators of essential services—including those in energy, health care, finance, transport, digital infrastructure, and telecommunications—are now subject to comprehensive cybersecurity compliance requirements. They must conduct regular assessments of cyber risks and implement both technical and organizational security measures, such as encryption protocols, multi-layered access controls, and secure data backups. A notable innovation is the legal requirement to appoint a designated information security officer (CISO or equivalent), who will be responsible for overseeing cybersecurity strategy and implementation. Entities are also obliged to develop formal incident response and business continuity plans, maintain internal logs of cyber incidents, and report significant incidents to the newly established Cybersecurity Agency and to GovCIRT within 24 hours of detection.

In addition to sector-specific obligations, the law introduces standardized risk management procedures and reporting frameworks that apply across the public and private sectors. Organizations falling under the law's scope are required to establish an Information Security Management System (ISMS), in alignment with internationally recognized ISO/IEC 27001 standard. Annual cybersecurity reports must be submitted to the competent regulatory authorities, and affected users must be notified if a breach compromises the confidentiality, availability, or integrity of their data or services. Public administration bodies, including central ministries and local municipalities, are also bound by a specific set of obligations. These include ensuring full legal and technical compliance of their information systems with the new regulatory framework, conducting annual internal cybersecurity audits, and providing mandatory staff training on digital hygiene and incident response.

Crucially, the law also creates new institutional structures. It mandates the formation of a dedicated Agency for Cybersecurity, which will serve as Montenegro's central authority for cyber defense.This Agency is envisioned as the lead actor for oversight and incident coordination, complementing the existing Government Computer Incident Response Team (GovCIRT) that is already operational.

Despite the adoption of the new cybersecurity law, significant gaps persist within the wider legal framework, particularly in areas such as data protection and institutional enforcement capacity, which may constrain the law's overall impact. It is important to note that Montenegro's current personal data protection law is antiquated and has not yet been brought into compliance with the EU's GDPR. The GDPR standards are not met by the current Law on Personal Data Protection, which was last amended in 2017. As a result, Montenegro's legislation lacks provisions for key GDPR rights such as data portability, clear conditions for consent, and mandatory data breach notification within 72 hours. These gaps significantly limit both the enforcement capacity of national authorities and the protection afforded to individuals, and they undermine public trust in digital services (BIRN, 2024).

Implementation Challenges

Montenegro's adoption of the 2024 Law on Information Security marks a substantial legal and policy alignment with the EU's cybersecurity acquis, particularly the NIS2 Directive. Yet, the successful operationalization of this framework poses a multilayered implementation challenge, requiring a shift from declarative compliance to sustained institutional performance. Core difficulties include the absence of mature cyber governance structures, fragmented operational roles across institutions, and insufficient cyber risk management integration at the organizational level. Many public entities and critical service providers lack embedded security architectures and standardized protocols for vulnerability assessment, incident handling, and business continuity. Moreover, the country's cybersecurity ecosystem suffers from a shortage of certified professionals, underdeveloped sectoral CERT functions, and limited automation in threat detection and response. These systemic limitations are reflected in Montenegro's standing on the ITU Global Cybersecurity Index 2024, where it ranks 97th globally, with a score of 46.62, indicating substantial gaps in strategic implementation, cyber resilience metrics, and interinstitutional coordination.

The formation of the national Cybersecurity Agency, as prescribed by the new legislation, will serve as a critical enabler for the broader regulatory architecture, but also as an immediate stress test. The agency's success will depend on its ability to exercise supervisory authority, coordinate with GovCIRT, and provide sector-specific guidance in accordance with international standards such as ISO/IEC 27001 and ENISA threat taxonomies. However, regulatory oversight is only one component; equally important is the agency's capacity to foster compliance readiness within critical infrastructure operators, including those in energy, telecommunications, transport, and financial services. These operators must undertake substantive upgrades in their security posture, including establishing designated security teams, implementing multi-layered defense mechanisms, formalizing incident response playbooks, and conducting regular penetration

testing and resilience drills. Without a deliberate and well-resourced implementation strategy, there is a risk that the legal framework remains underutilized, delaying Montenegro's convergence with EU cybersecurity norms and leaving critical assets exposed to increasingly sophisticated threat actors.

A particular focus is needed on small and medium-sized enterprises (SMEs), which make up the backbone of Montenegro's economy – and often its weakest link in cybersecurity. Montenegro has over 45,000 active business entities, and *99.2%* of them are small businesses. SMEs account for roughly *80% of total employment* in the country, meaning any widespread cyber vulnerabilities in the SME sector pose systemic economic risks (Montenegro Business, 2024). This is not just a Montenegrin problem: globally, *90%* of businesses are SMEs and they are often the least able to tackle cyber threats. They may lack dedicated IT security staff, have limited budgets for security tools, and provide minimal training to employees (Arroyabe et al.,2024). Consequently, cybercriminals increasingly target SMEs, knowing these firms are softer targets. A recent global survey found that 46% of SMEs have experienced a cyberattack, and alarmingly, nearly one in five of those attacked ended up filing for bankruptcy or closing their business. The aftermath of attacks is especially devastating for small businesses – lost data, financial fraud, or ransomware payments can cripple their finances, and 80% of attacked SMEs report having to spend significant effort to rebuild trust with customers (Gerber & Prokop, 2025).

For Montenegrin SMEs, there is a prevailing misconception among small business owners that they are "too small to be noticed" by hackers – a dangerous myth that recent trends have debunked. The new Information Security Law will likely impose certain obligations on operators of essential services and possibly digital service providers, some of which could be SMEs. The complexity of legal requirements, combined with insufficient financial capacity for audits or upgrades, further exacerbates the risk of non-compliance. Without targeted support, these limitations may undermine implementation and widen gaps in national cyber resilience.

Therefore, the Montenegrin government, in implementing the law, may consider initiatives specifically tailored to SMEs: e.g. simplified security guidelines, free or subsidized cybersecurity audits, and training programs. In parallel with raising awareness, it is essential to strengthen mechanisms for reporting cybersecurity incidents. Citizens and businesses must clearly understand where and how to report a cyberattack or a suspected security breach. Establishing a single reporting point, such as an online portal or dedicated phone line and actively promoting it would improve responsiveness, especially if accompanied by assurances that reporting will not result in penalties but rather trigger assistance. Transparency in incident response is equally important; institutions should regularly publish aggregated data on the number and types of incidents and the measures taken in response, thereby building public trust. Furthermore, in developing all new digital services and e-government platforms, the principle of "privacy by design" should be applied—meaning that privacy safeguards must be integrated from the earliest stages of system planning. In the EU, some countries have created SME-focused cybersecurity support centers as a good practice, recognizing that the overall cyber resilience of a nation hinges on not only fortifying government systems but also uplifting smaller enterprises. Ultimately, Montenegro's cybersecurity is only as strong as its weakest links and unless SMEs are brought up to speed, they will remain highly vulnerable in the face of rising cyber threats.

European Trends and Best Practices

From a comparative perspective, there are notable European trends and best practices that Montenegro can draw upon as it strengthens its cybersecurity framework. One often-cited example is Estonia, a small nation like Montenegro that endured a massive cyber assault in 2007 and then became a world leader in cybersecurity. Through consistent investment in cyber defenses, public awareness, and international cooperation, Estonia now ranks among the top countries globally in cybersecurity readiness (8th worldwide in the ITU's Global Cybersecurity Index). It has a dedicated cyber command, digital ID system, and hosts the NATO Cyber Defence Centre of Excellence – all contributing to a reputation for cyber resilience. While Estonia's context differs, it shows that *size is not destiny*: even a small country can build a strong cybersecurity posture with political will and expertise. Countries like Finland, the Netherlands, and Germany have institutionalized cybersecurity not only as a technical function but as a core component of national resilience, closely linked to education, innovation policy, and civil protection. For example, Finland's "whole-of-society" approach emphasizes preparedness exercises that include municipalities, businesses, and civil society actors. The Netherlands has established a national cybersecurity alliance that brings together government agencies, academia, and industry to jointly define priorities and share intelligence. These models demonstrate the importance of multi-stakeholder collaboration, decentralization with coordination, and sustained political commitment. In the Western Balkans region, countries are increasingly collaborating on cyber issues – sharing threat intelligence and training through regional forums. Adopting international best practices – from ISO 27001 information security standard to organizational models (like sectoral Computer Emergency Response Teams and public-private information

sharing groups) will accelerate Montenegro's progress.

Conclusion

Montenegro's new Law on Information Security represents a pivotal move towards fortifying the nation's cyber defenses and aligning with European norms. The law introduces much-needed structure into a previously under-regulated domain, bringing Montenegro closer to EU cybersecurity standards and NATO best practices. If implemented effectively, it can significantly improve national resilience: critical infrastructure will be better protected, breaches will be managed in a coordinated way, and a culture of cybersecurity could take root across government and industry. However, the journey from law to reality is fraught with challenges. Montenegro must rapidly build up its institutional capacity, equipping the nascent Cybersecurity Agency with skilled personnel, clear procedures, and the authority and trust to act. It must also invest in its people: training a new cadre of cybersecurity experts, upskilling law enforcement and IT professionals, and raising awareness among end-users. Given that SMEs form the majority of Montenegrin enterprises, special focus on helping small businesses improve their cybersecurity is essential to the law's success. Moreover, the legal framework will need to be completed by addressing related areas like data protection (aligning with GDPR) and updating cybercrime statutes, to ensure consistency and comprehensive coverage.

Montenegro's readiness for this digital security overhaul is nascent, but not without support. The EU, through its progress monitoring and instrument funds, and NATO allies are already providing expertise and resources to shore up Montenegro's cyber capabilities. Such international cooperation can help bridge the skills and technology gaps in the short term. In the longer term, Montenegro will want to foster a homegrown ecosystem of cybersecurity – including academic programs, industry initiatives, and maybe even cyber startups – to sustain its defenses. The stakes are high: as Montenegro moves toward deeper EU integration and digital transformation, its exposure to cyber threats will only increase. Ensuring the security of networks, data, and critical services is not only about EU membership conditionality, but about protecting Montenegro's economy, privacy of citizens, and national security in the digital age. With strong commitment and smart implementation, the new Information Security Law can be a catalyst for Montenegro to leap forward into a safer cyber future, turning what is now a vulnerable landscape into one of resilience and trust.

Arroyabe, M. F., Arranz, C. F. A., Fernández de Arroyabe, I., & Fernández de Arroyabe, J. C. (2024). Revealing the realities of cybercrime in small and medium enterprises: Understanding fear and taxonomic perspectives. *Computers & Security, 141*, 103826. https://doi.org/10.1016/j.cose.2024.103826

Balkan Investigative Reporting Network (BIRN). (2024). *Cyber-security capacities and digital rights in Montenegro* (p. 2). https://birn.eu.com

Council of Europe. (2001). *Convention on Cybercrime (CETS No. 185)*. https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185 (Accessed: July 03, 2025)

Council of Europe. (2024, January). *Cybercrime@CoE Update: October – December 2023 (Q4/2023)*. https://rm.coe.int/cybercrime-coe-update-q4-2023/1680ae5489

European Commission. (2022). *Commission Staff Working Document: Montenegro 2022 Report. Accompanying the document Communication on EU Enlargement Policy*. Brussels: European Commission. https://enlargement.ec.europa.eu/system/files/2022-10/Montenegro%20Report%202022.pdf

European Commission. (2023). *Enlargement Package 2024*. https://enlargement.ec.europa.eu (Accessed: July 04, 2025)

European Union Agency for Cybersecurity (ENISA). (2023). *ENISA Threat Landscape 2023 – Overall Threat Assessment*. Athens: ENISA.

Gerber, J., & Prokop, J. (2025, March 27). Small business cybersecurity: Survey shows reason for worry. *Mastercard*. https://www.mastercard.com/us/en/news-and-trends/stories/2025/small-business-cybersecurity-study.html (Accessed: July 07, 2025)

Global Initiative Against Transnational Organized Crime. (2024, April 4). *Cyber-enabled crime poses significant risks to South Eastern Europe. Risk Bulletin – South Eastern Europe Observatory*, (19). https://riskbulletins.globalinitiative.net/see-obs-019/01-cyber-enabled-crime-south-eastern-europe.html

Hasan, M. T. (2024). Cross-border cybercrimes and international law: Challenges in ensuring justice in a digitally connected world. *IJRDO Journal of Law and Cyber Crime*, 4(1), 1–7.

International Telecommunication Union (ITU). (2024). *Global Cybersecurity Index 2024: Enhancing Digital Trust*. Geneva: ITU. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx (Accessed: July 05, 2025)

Montenegro Business. (2023, April 2). The number of business entities in Montenegro last year was 45.68 thousand. https://montenegrobusiness.eu/the-number-of-business-entities-in-montenegro-last-year-was-45-68-thousand (Accessed: July 05, 2025)

Reuters. (2022, September 1). Montenegro blames criminal gang for cyber attacks on government. https://www.reuters.com/world/europe/montenegro-blames-criminal-gang-cyber-attacks-government-2022-08-31/#:~:text=,Dukaj%20said (Accessed: July 03, 2025)

Western Balkan Cyber Capacity Centre (WB3C). (2025). https://wb3c.org/

World Economic Forum (WEF). (2025, January). *How AI-driven fraud challenges the global economy—and ways to combat it*. https://www.weforum.org/stories/2025/01/how-ai-driven-fraud-challenges-the-global-economy-and-ways-to-combat-it/ (Accessed: July 05, 2025)

Improving EU Cybersecurity Resilience: An in-depth analysis of ENISA's Cyber Stress Test Handbook

In an increasingly interconnected and digitally dependent world, the resilience of critical infrastructure against cyber threats has become a paramount concern for nations and unions alike. The European Union, through its dedicated agency, ENISA (the European Union Agency for Cybersecurity), is at the forefront of developing robust strategies and tools to bolster this resilience. A significant contribution to this effort is ENISA's „Handbook for Cyber Stress Tests," a draft published in Mai 2025. This comprehensive guide outlines a novel, lightweight, and targeted approach to assessing cybersecurity and resilience, offering a vital new instrument in the toolkit of national authorities.

The concept of stress tests gained prominence in the financial sector following the 2007–2009 global financial crisis, where they were used to evaluate banks' ability to withstand severe financial shocks. ENISA has adapted this methodology to the cybersecurity domain. The handbook defines a cyber stress test as:

> „a targeted assessment of the resilience of individual organisations and their ability to withstand and recover from significant cybersecurity incidents, ensuring the provision of critical services, in different risk scenarios." (ENISA, 2025, p. 7 [1])

It is crucial to understand what a cyber stress test is *not*. According to the handbook, it is distinct from a penetration test (a live simulation of an attack), it is not conducted in real-time, and it differs from a cyber exercise (which tests operational collaboration between multiple entities, whereas stress tests are individual and independent) (ENISA, 2025, p. 7-8). This distinction highlights the unique utility of cyber stress tests as a focused, analytical tool.

Core Characteristics of Cyber Stress Tests

The handbook outlines six key characteristics that define cyber stress tests:

1. **Resilience focus:** These tests are designed to evaluate an organization's resilience against various cyber threats, serving as tools to identify failure points and improve preparedness, response, and recovery.
2. **Scenario-based:** They adopt a „what if" approach, utilizing plausible and realistic risk scenarios.
3. **Stress levels:** Different severity levels are incorporated into the tests, including „black swan" events (low-probability, high-impact incidents), to gauge an organization's preparedness under escalating pressure.
4. **Resilience metrics:** Both qualitative and quantitative metrics, such as „time-to-detect" and „time-to-recover," are employed to objectively measure resilience.
5. **Individual and independent:** Organizations carry out these tests independently, typically by completing detailed technical questionnaires.
6. **Systemic risk view:** Cyber stress tests aim to identify cascading effects and interdependencies across a sector, providing a broader understanding of systemic risks (ENISA, 2025, p. 7,[1]).

A Step-by-Step Guide to Implementation

The handbook provides a clear, five-step guide for organizing a cyber stress test:

1. **Define scope and objectives, engage with stakeholders:** This initial phase involves identifying the specific sector, entities, and ICT infrastructure to be tested. It also requires formulating clear test objectives and selecting high-level risk scenarios. Crucially, relevant stakeholders (e.g., non-cyber authorities, sector-specific experts, CSIRT teams, law enforcement) must be engaged to provide valuable domain knowledge and benefit from the test outcomes. The report suggests forming a steering board or oversight committee with these stakeholders (ENISA, 2025, p. 11-12).
2. **Design the test, choosing the methodology, refining the scenarios:** This step focuses on selecting the appropriate testing methodology, which is typically a desktop-based technical questionnaire. High-level risk scenarios are refined to include specific infrastructure, business processes, IT architecture, and ICT systems. The concept of „escalation" in scenario development is highlighted, where severity can be increased by scaling impact or layering multiple scenarios (ENISA, 2025, p. 13).
3. **Execution of the cyber stress test:** This involves the entities independently completing the assessment, often through the provided questionnaire.
4. **Analysing results and identifying gaps:** Once data is collected, authorities analyze the responses to identify

areas of weakness and potential vulnerabilities.

5. **Recommendations and following up on gaps and issues identified in the stress test:** The final step involves addressing the discovered shortcomings, which can be done through collaborative discussions or, if deemed necessary, within a stricter supervisory framework (ENISA, 2025, p. 10).

Policy Alignment and Future Outlook

The „Handbook for Cyber Stress Tests" is firmly rooted in the current EU policy context, reflecting the Union's intensified focus on preparedness and resilience. It aligns with several key initiatives such as the NIS2 Directive, Union risk evaluations, Cyber Solidarity Act (CSoA) and etc (ENISA, 2025, p. 5-6). In conclusion, ENISA's „Handbook for Cyber Stress Tests" represents a significant step forward in the EU's efforts to cultivate a robust and resilient digital ecosystem. By providing a structured, adaptable, and collaborative framework for assessing cybersecurity preparedness, this handbook empowers national authorities to proactively identify and address vulnerabilities, ultimately strengthening the Union's collective ability to withstand the evolving landscape of cyber threats. As the NIS2 Directive concludes its transposition, cyber stress tests are poised to become an indispensable tool for ensuring Europe's digital security.

Bibliography:

1. European Union Agency for Cybersecurity (ENISA). (2025, May). *Handbook for Cyber Stress Tests* (Draft, April 2025). Retrieved June 2, 2025, from https://www.enisa.europa.eu/sites/default/files/2025-05/2025.04311_01_ms_v2.0_Handbook%20for%20Cyber%20Stress%20Tests_en.pdf

PROJECT NEWS

CSUPMNE project represented at Media Day 2025

Media Day 2025, held on May 29 at the University of Maribor, Faculty of Electrical Engineering and Computer Science (FERI), brought together students, academic staff, and industry representatives to celebrate media, communication, and creativity. Organized by the Institute for Media Communication, the event offered a dynamic platform to explore trends in media production, visual communication, marketing, and related fields.

A key part of the event was the project exhibition, featuring various student and staff initiatives aimed at promoting innovation and strengthening connections between academia and industry.

Among the showcased projects was CSUPMNE, which focuses on enhancing cybersecurity awareness and practices in Montenegro's media sector. The presentation highlighted the project's main objectives, planned activities, and initial implementation steps, sparking strong interest by emphasizing the importance of cybersecurity for sustainable development and digital innovation in the region.

Overall, Media Day 2025 successfully emphasized the value of collaboration, creativity, and forward-looking approaches in shaping the media landscape.

From Vulnerability to Resilience: Enhancing Cybersecurity in Montenegro's Private Higher Education via CSupMNE

Prof. dr Radislav Jovovic, University Mediterranean

Prof. dr Marija Jankovic, University Mediterranean

Private universities in Montenegro play an increasingly important role in the country's higher education system, offering specialized programs and attracting both local and international students. As these institutions digitize their operations—adopting online platforms, digital libraries, remote learning tools, and student management systems—they also become more vulnerable to cyber threats. However, unlike larger public institutions, private universities often face a distinct set of cybersecurity challenges shaped by their size, structure, and limited resources (ENISA, 2022). This paper analyses the main challenges and contribution of Erasmus project CSupMNE for overcoming them.

1. Challenges

Limited Budgets and Prioritization Issues. Private universities in Montenegro typically operate with tight budgets, and much of their financial focus is on attracting students, expanding programs, and covering operational costs. Cybersecurity is often not prioritized unless a serious breach has already occurred (Ponemon Institute, 2021). Investing in firewalls, intrusion detection systems, secure backup solutions, or even routine software upgrades may be viewed as secondary to academic marketing or infrastructure improvements.

Lack of Specialized Cybersecurity Personnel. Most private universities do not have dedicated cybersecurity professionals. Instead, general IT staff—often small in number—handle everything from computer maintenance to system administration. These staff members may not have up-to-date training or knowledge of modern cyber threats or risk mitigation techniques (Sucuoğlu & Tunc, 2022). This leads to a reactive rather than proactive approach. Without formal monitoring or response strategies, even basic threats like phishing emails or ransomware can cause widespread disruption (OECD, 2020).

Outdated Infrastructure and Software. Many private universities continue to rely on outdated software platforms for student records, e-learning systems, and internal communication. These legacy systems are often vulnerable to exploits and lack proper encryption or access controls. The use of pirated or unlicensed software—still an issue in some institutions—exposes networks to considerable risk (Halili & Gashi, 2020). Open Wi-Fi networks and bring-your-own-device (BYOD) policies further complicate cybersecurity efforts, as they increase the number of potential entry points for attackers (Gokhale & Andhale, 2021).

Weak Cyber Hygiene Among Students and Staff. Cybersecurity awareness among students, faculty, and administrative staff remains very low across most private universities. Password sharing, weak authentication practices, and a lack of awareness about phishing scams increase vulnerability (ENISA, 2022). Without institutional training programs or awareness campaigns, most users are unprepared to recognize suspicious activity, respond to incidents, or even report security issues (Ponemon Institute, 2021).

Regulatory Compliance and Data Protection Risks. With increasing expectations around data protection—especially under European standards like the GDPR—private universities are under growing pressure to protect personal and academic data (European Commission, 2023). However, many lack clear internal policies on data handling, encryption, and breach reporting. This is concerning given the large amount of sensitive data managed by universities, including academic records, payment details, and even biometric data (UNDP, 2023).

Exposure to Reputation-Damaging Attacks. Unlike their public counterparts, private universities operate in a competitive environment where reputation is closely tied to student trust and enrollment. A cybersecurity incident—such as a ransomware attack or data breach—can have a disproportionate impact on credibility and financial stability (Janković & Milačić, 2021). Reputational risks often exceed the direct financial costs of a breach,

making proactive cybersecurity policies a strategic necessity.

2. The Role of the Erasmus+ CSupMNE Project in Enhancing Cybersecurity

The Erasmus+ project **CSupMNE (Cyber Security for Universities in Montenegro)** offers significant potential to strengthen cybersecurity in Montenegro's private higher education sector. It directly addresses the key vulnerabilities outlined above by providing both strategic and practical support.

First, CSupMNE contributes to **institutional capacity building**. Through policy development, it helps private universities establish formal cybersecurity frameworks, risk mitigation protocols, and response plans. These foundations are critical for small institutions lacking internal governance mechanisms.

Second, it supports **curriculum development and modernization** by enabling private universities to integrate cybersecurity content into IT, engineering, and business programs. This fosters a new generation of graduates with relevant digital security competencies.

Third, the project facilitates **training and professional development** for teaching and technical staff, introducing them to up-to-date tools and techniques via workshops, mobility programs, and collaboration with EU partner universities. For institutions with minimal or generalist IT staff, this is transformative.

Moreover, CSupMNE promotes **cybersecurity awareness among students**, encouraging the creation of student-led initiatives, awareness campaigns, and digital safety workshops. These interventions help instill a culture of security and responsibility throughout the academic community.

Finally, the project strengthens **international collaboration**, enabling private universities to access European best practices, learning materials, and networks that would otherwise be out of reach. This promotes alignment with EU cybersecurity norms and accelerates digital readiness (European Commission, 2023).

Conclusion

For private universities in Montenegro, cybersecurity is not simply a technical issue—it is a strategic imperative. The shift toward digital learning, online services, and data-driven administration requires strong, institutional-level commitments to protecting digital infrastructure. Even with limited resources, practical steps and awareness can help private institutions build digital trust and resilience in an increasingly connected academic environment.

The CSupMNE project, by offering structured support in education, training, policy, and regional cooperation, provides a unique opportunity for private universities to overcome their cybersecurity limitations and better protect their communities in the digital era.

References

1. ENISA (2022). *Threat Landscape for Education Sector*. European Union Agency for Cybersecurity. Retrieved from https://www.enisa.europa.eu
2. Ponemon Institute (2021). *The State of Cybersecurity in Higher Education*. Retrieved from https://www.ponemon.org
3. OECD (2020). *Digitalisation in Higher Education: Challenges and Opportunities*. OECD Publishing. https://www.oecd.org
4. Sucuoğlu, M., & Tunc, H. (2022). "Cybersecurity Capacity in Small Institutions: Issues in Human Capital." *Journal of Cybersecurity Education*, 4(1), 45–59.
5. Halili, R., & Gashi, B. (2020). "Cybersecurity in Higher Education in the Western Balkans: Current State and Risks." *Western Balkan IT Review*, 12(2), 22–31.
6. Gokhale, S., & Andhale, R. (2021). "BYOD and Its Challenges in University Networks." *International Journal of Network Security*, 23(1), 1–7.
7. European Commission (2023). *General Data Protection Regulation (GDPR) Compliance Guidelines for Higher Education Institutions*. https://ec.europa.eu
8. Janković, S., & Milačić, N. (2021). "Cybersecurity as a Reputational Risk in Private Higher Education." *South-East European Journal of Economics and Business*, 16(1), 89–98.
9. UNDP Montenegro (2023). *Digital Transformation and Data Security in the Montenegrin Education Sector: Risk Assessment Report*. https://www.me.undp.org
10. CSUPMNE Project Consortium (2024). *Cyber Security for Universities in Montenegro – Project Goals and Expected Outcomes*. Erasmus+ CBHE Project Brief. Retrieved from https://csupmne.ucg.ac.me
11. European Commission (2024). *Erasmus+ Capacity Building in Higher Education: Project Database*. Retrieved from https://erasmus-plus.ec.europa.eu

MontEDIH - Synergy Between Science and Business is Key to Creating Market-Sustainable Innovations Compromise

The Chamber of Economy of Montenegro organized first promotion and info day of the MontEDIH project. The project budget is approximately two million euros. It is co-financed by the European Union (50%) through the "Digital Europe" programme, the Government of Montenegro (45%), and the project consortium (5%). Project name is: Digital innovation hub for supporting the digital transformation of Montenegrin companies and the public sector.

MontEDIH, which is the first and unique Montenegrin European Digital Innovation Hub is now available to small and medium-sized enterprises and public administration. It will enable easier access to innovative and digital tools, knowledge, and expertise from various fields, thereby strengthening the competitiveness, productivity, and sustainability of the Montenegrin economy and the efficiency of public administration.

MontEDIH offers companies and institutions the opportunity to enhance their resilience to market challenges, use resources more efficiently, and become part of the European digital community. MontEDIH is part of a network of more than 150 European Digital Innovation Hubs (EDIHs).

The project is coordinated by the Faculty of Electrical Engineering of the University of Montenegro, and the consortium includes the Chamber of Economy, the University of Donja Gorica, the Institute of Contemporary Technologies of Montenegro, the Innovation and Entrepreneurship Center Tehnopolis – Nikšić, the Science and Technology Park of Montenegro, Center for Finance LLC Podgorica, and ICT Cortex. Consortium members presented the services and tools available to users through the Digital Innovation Hub, which are detailed on the website www.montedih.me.

The synergy between research institutions and the business sector, theory and practice, will be key to creating applicable and market-sustainable innovations. MontEDIH will contribute not only to innovation development but also to fostering an innovation culture, helping young but already recognized national institutions of innovation infrastructure grow further.

MontEDIH is a platform for collaboration that erases the boundaries between science and business, between academic institutions and system entities. All services offered by MontEDIH will be freely available during the project's duration.

MontEDIH is not just another European project – it is a powerful example of a partnership-based approach that unites the best from academia, innovation infrastructure, and the business sector.

Representatives of CSupMNE Montenegrin partners take part at the MOntEDIH info day. They used this opportunity to network with representatives of other institutions and the business sector, introducing them to the goals and activities of this important project, which addresses key issues of cybersecurity in higher education.

Training in Kraków: Sharing Experience and Knowledge Transfer with Polish CERT

On April 8–9, 2025, AGH University of Kraków hosted a training event titled "Sharing Experience and Knowledge Transfer with Polish CERT" as part of the CSupMNE project. The event focused on supporting Montenegro in the development of national frameworks for cybersecurity in the academic sector. It aimed to transfer Polish experience in establishing and operating CERT/CSIRT units, developing interdisciplinary cybersecurity education, and integrating practical tools into institutional cybersecurity infrastructures. The training was led by specialists from AGH University's Centre for Information Security (CBI), one of the most recognized academic cybersecurity hubs in Poland. Guest speakers from the Ministry of National Defence and the Cybersecurity Foundation also provided valuable insights into national cybersecurity strategies and education policies.

The Montenegrin delegation consisted of representatives from major universities (University of Donja Gorica, University of Montenegro, Mediterranean University, Adriatik University Bar), government bodies (Agency for Control and Quality Assurance of Higher Education, Institute of Modern Technologies), and the Chamber of Economy. This diverse group brought a mix of technical, academic, and regulatory expertise, ensuring that the training would have a wide-ranging institutional impact.

The program combined theoretical foundations with practical demonstrations and collaborative discussions. Participants were introduced to the structure of CERT teams in Poland, including the NASK model and ECSC training initiatives. They explored tools such as the SOC4Academia toolbox, a key resource for establishing academic Security Operation Centers (SOCs). The training also emphasized curriculum development aligned with European standards, particularly ENISA's CYBERHEAD database and the EU Cybersecurity Skills Academy.

A key highlight of the event was the CyberBastion simulation - a serious board game used for training in cybersecurity decision-making. Participants also toured AGH's specialized cybersecurity facilities, observed real-time threat monitoring and vulnerability scanning, and learned how Polish academic institutions manage cybersecurity incidents. These activities helped bridge the gap between policy and practice, offering attendees a first-hand experience of operating a university-based SOC.

UPCOMING EVENTS & ANNOUNCEMENTS

One of the goals of the CSupMNE project is to inform the general public about the project's goals, as well as to raise awareness of the importance of cybersecurity in the modern world. To this end, the project envisages 3 major (Community Building) events each year, where the first such (networking) event is planned to be held in October. The National Networking Event will be organized by the partner AUB from Budva, and it is planned as a come-together for national stakeholders with a minimum of 30 external participants..

The next event is the Sustainability Event. It is planned that all project participants will be part of roundtable on selected topics in the field of cybersecurity with 20 external participants.

One of the most important and largest event in Montenegro in the field of cybersecurity will be the Annual Project Conference. This event will be held in Podgorica and is planned to be attended by at least 100 external participants (50 on-site, 50 online). The aim of the conference is to create an impact in the academic and business communities, to disseminate the project and to facilitate connection with the industry and other associations interested in cyber security.

After the training in Krakow in April this year, the next workshop, entitled as CSIRT service portfolio, is planned to be held in Maribor, Slovenia, in the last week of August. The workshop will be part of the efforts of the CSIRT establishment process.