CSupMNE
Straightening Up Cybersecurity Posture of Montenegrin Higher Education system

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

issue# 5, August 2026

newsletter

WORD OF THE EDITOR

Cyber resilience begins with people, knowledge, and continuous practice. In this issue, we explore how higher education institutions can strengthen their cybersecurity posture by combining modern regulatory requirements with practical capacity building. From understanding the implications of the EU Cyber Resilience Act for universities to address the growing cybersecurity skills gap, this edition highlights that resilient institutions are built through well-prepared people as much as through technology.

Cybersecurity is becoming a strategic responsibility for every higher education institution. New European legislation, evolving cyber threats, and increasing dependence on digital services require universities to strengthen governance, develop secure software, invest in skilled professionals, and regularly test their ability to respond to incidents. Ljubljana.

Inside this issue, you will find:

Featured: Navigating the EU Cyber Resilience Act – practical guidance on what the CRA means for universities and research organisations.

Short: The Empty Fortress – why developing cybersecurity talent is essential for Montenegro's digital resilience.

Update: Hands-on Protect training in Schwenningen, where participants translated governance principles into practical security controls, incident response, and institutional action plans.

Upcoming Events: Opportunities to meet the CSupMNE project team at INFOFEST 2026 and the Economic Conference Montenegro 2026.

Project Highlights: The latest project achievements, capacity-building activities, collaborative events, and upcoming initiatives.

I would also like to express my sincere gratitude to all our project partners. Your expertise, commitment, and valuable contributions have made this issue possible and continue to strengthen the CSupMNE project and its mission of enhancing cybersecurity capacities in higher education.

We hope you enjoy this edition and find ideas that you can apply within your own institution.

Contents:

2 **Navigating the EU Cyber Resilience Act: Implications for Universities and Research Organisations**

5 **The Empty Fortress – Securing Montenegro's digital future starts with people, not just laws**

6 **Protect in Practice: Hands-On Incident Management and Restoration Training in Schwenningen**

8 **Upcoming events:**
I: MontEDIH and CSupMNE to Be Presented at INFOFEST 2026
II: Visit the MontEDIH Info Corner at the Economic Conference Montenegro 2026

9 **CSupMNE Partners Strengthen Cybersecurity Capacities through Hands-On Training at Furtwangen University**

11 **CSupMNE Project Presented at International Days 2026**

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.

Navigating the EU Cyber Resilience Act: Implications for Universities and Research Organisations

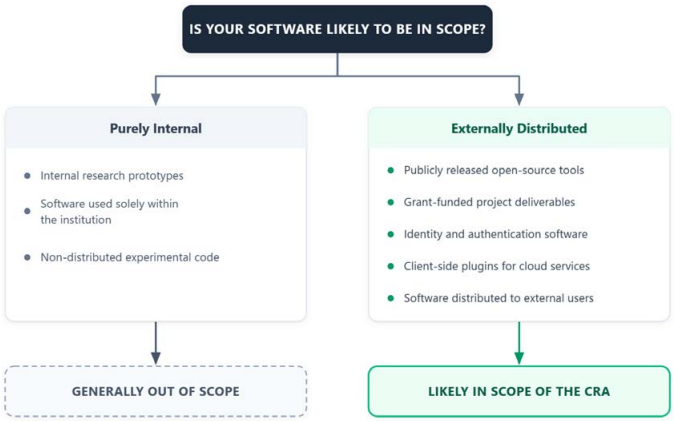
Dr Branko Marović, University of Belgrade

The Cyber Resilience Act (CRA), Regulation (EU) 2024/2847, establishes a new regulatory framework for the cybersecurity of products with digital elements placed on the European market. Unlike earlier European cybersecurity legislation, most notably the NIS2 Directive, which regulates operators of essential and important entities, the CRA regulates software and hardware products themselves by imposing mandatory cybersecurity requirements throughout their lifecycle. Security therefore becomes a legal obligation extending from product design through maintenance, vulnerability management, and end-of-support.

Although early discussion of the CRA focused primarily on commercial technology vendors, the Regulation also has significant implications for higher education institutions (HEIs) and research organisations. Universities increasingly develop, maintain, distribute, and govern software that is used beyond their own organisational boundaries, including research platforms, identity-management systems, scientific applications, learning technologies, and research infrastructures. Consequently, many institutions may fall within the Regulation's scope despite operating on a non-profit basis.

Scope and Applicability

The CRA applies to **products with digital elements (PDEs)**, defined as software or hardware, together with associated remote data-processing components where applicable, that is made available to third parties. Software developed solely for internal organisational use or retained exclusively within research projects generally falls outside the Regulation's scope. Likewise, software-as-a-service without a distributed client component is excluded, although locally installed clients, plugins, libraries, or desktop agents accompanying cloud services remain subject to the Regulation.



Scope of the Cyber Resilience Act for software eveloped by higher education institutions.

Whether academic software falls within the CRA depends primarily on whether it is made available beyond the developing institution and whether that activity has a commercial dimension. The concept of **commercial activity is interpreted broadly** and is not limited to conventional software sales. Software distributed under publicly funded research programmes, maintained through paid support arrangements, transferred via technology-transfer offices, or provided as shared infrastructure across multiple institutions may therefore be subject to the Regulation. Typical examples include open-source scientific software, research platforms, identity-management services, authentication frameworks, collaborative infrastructure, and deployable client components accompanying cloud services.

Regulatory Roles

An institution's legal obligations under the CRA depend on how it develops, governs, and distributes its software.

Institutional Role	CRA Definition and Context	Primary Legal and Technical Obligations
Manufacturer	Develops and places a PDE on the market under its own name or trademark.	Cybersecurity risk assessment, technical documentation, Software Bills of Materials (SBOMs), conformity assessment, an EU Declaration of Conformity, CE marking where applicable, and declaration of an appropriate support period (five years by default unless another period is justified).
Open Source Software (OSS) Steward	Systematically supports and governs open-source software intended for broader use without directly commercialising it.	Documented cybersecurity policies, coordinated vulnerability disclosure procedures, and reporting obligations. Exempt from conformity assessment, CE marking, and administrative fines.
Distributor	Redistributes third-party software without making substantial functional modifications.	Must verify that the manufacturer has fulfilled the applicable regulatory requirements, including conformity assessment and CE marking, where applicable, before making products available further along the supply chain.

Regulatory Timeline

The CRA is implemented through a phased schedule. Several milestones are particularly relevant for universities and research organisations:



Phased implementation timeline of the Cyber Resilience Act (2024–2027).

The Regulation entered into force on **10 December 2024**, while provisions governing the designation of conformity assessment bodies became applicable on **11 June 2026**. The first major operational obligations arise on **11 September 2026**, when manufacturers and OSS stewards become subject to mandatory reporting requirements for actively exploited vulnerabilities and severe security incidents through the ENISA Single Reporting Platform (SRP). These obligations apply not only to newly released products but also to software already placed on the market. Full application of the Regulation, including conformity assessment and CE marking requirements, where applicable, begins on **11 December 2027**.

Principal Compliance Requirements

The CRA establishes substantive cybersecurity requirements primarily through Annex I and accompanying technical documentation obligations set out in Annex VII.

Manufacturers must incorporate cybersecurity throughout the **software lifecycle** by implementing **security-by-design** and **security-by-default** principles. These include secure authentication, protection of data both at rest and in transit, secure update mechanisms, vulnerability management processes, and measures intended to minimise attack surfaces. For each in-scope product, manufacturers must also prepare comprehensive **technical documentation** covering system architecture, cybersecurity risk assessment, vulnerability management procedures, lifecycle support planning, and Software Bills of Materials (SBOMs).

The Regulation further distinguishes products according to risk. Most research software falls within the **default (low-risk)** category and may be assessed through internal conformity assessment procedures. However, products performing security-sensitive functions, including identity-management systems and network-monitoring software, may fall within the **Class I (important)** category, potentially requiring **third-party conformity assessment** where harmonised European standards are not applied. Third-party conformity assessment is mandatory for **Class II (important)** and **critical** products, including infrastructure software such as hypervisors, firewalls, intrusion detection and prevention systems, and hardware security modules (HSMs).

Incident Reporting and Vulnerability Management

Among the CRA's most operationally significant provisions is its incident-reporting framework. From **11 September 2026**, manufacturers and, where applicable, open-source software stewards become responsible for reporting actively exploited vulnerabilities and severe security incidents affecting products with digital elements through the ENISA Single Reporting Platform (SRP). The platform serves as a central reporting mechanism, forwarding notifications to the relevant national Computer Security Incident Response Teams (CSIRTs) and other competent authorities.

The reporting process follows a staged approach intended to balance rapid notification with the availability of technical information. An **initial early warning must be submitted within 24 hours** of becoming aware of an actively exploited vulnerability or severe security incident. A **more detailed notification is required within 72 hours**, providing an initial technical assessment, the likely impact, and any mitigation measures already implemented. A **final report must be submitted within 14 days** of a corrective measure becoming available for an actively exploited vulnerability, or within one month of the 72-hour notification for severe security incidents. Significantly, these obligations extend not only to newly released products but also to software already placed on the market before the reporting regime becomes applicable.

Third-Party Software and Supply-Chain Responsibility

The CRA has implications not only for software developed within universities but also for software acquired from commercial suppliers, research partners, and open-source communities. Although the principal legal obligations generally rest with the manufacturer or open-source software steward, institutions remain responsible for

selecting, deploying, and operating software securely.

For **commercial software**, procurement and contract-management processes are likely to place increasing emphasis on cybersecurity alongside traditional considerations such as functionality, cost, and licensing. Institutions should seek assurance that suppliers maintain appropriate vulnerability-management processes, provide security updates throughout the declared support period, and comply with the applicable CRA requirements, including conformity assessment, CE marking where required, and the availability of an EU Declaration of Conformity.

Open-source software presents different, although equally significant, considerations. Modern research software commonly incorporates numerous third-party libraries, often through extensive dependency chains. While the CRA does not alter the fundamental importance of open source to research and innovation, it reinforces the need for institutions to evaluate the governance, maintenance activity, release frequency, vulnerability response processes, community sustainability, and security documentation of externally developed software before adopting it in production systems.

Where an institution distributes software incorporating third-party open-source components, responsibility does not end with the upstream project. Vulnerabilities affecting embedded dependencies may require action by the distributing institution regardless of whether the original maintainers have released corrective updates. Consequently, software composition analysis (SCA), continuous dependency monitoring, vulnerability scanning, SBOM generation and maintenance, and timely patch management become important components of an effective software lifecycle management. Although these practices represent established software engineering principles, the CRA places them within a clear regulatory framework.

Strategic Considerations for Higher Education Institutions

The CRA requires universities and research organisations to develop a more systematic understanding of the software they produce and distribute. An initial priority is the identification of products that qualify as products with digital elements and the determination of the institution's regulatory role as manufacturer, open-source software steward, or distributor. These responsibilities should be integrated into existing institutional governance frameworks alongside related obligations arising from the NIS2 Directive, the General Data Protection Regulation (GDPR), and information security management frameworks such as ISO/IEC 27001.

Institutions should also establish formal coordinated vulnerability disclosure procedures, ensuring that security researchers and users have clearly defined mechanisms for reporting vulnerabilities. Designating responsible security contacts for major software projects and ensuring appropriate access to the ENISA Single Reporting Platform will facilitate compliance with the reporting obligations introduced in September 2026. At the technical level, integrating automated SBOM generation, vulnerability assessment, and dependency analysis into continuous integration and continuous deployment (CI/CD) pipelines can significantly improve software supply-chain visibility while supporting regulatory compliance.

These measures should not be viewed solely as mechanisms for satisfying legal obligations. Rather, they contribute to improving software quality, increasing transparency throughout the software lifecycle, and strengthening institutional capability to manage cybersecurity risks within increasingly complex research software ecosystems.

Concluding Remarks

The Cyber Resilience Act represents a significant evolution in European cybersecurity regulation by extending legally enforceable cybersecurity obligations to software and hardware products throughout their lifecycle. Its scope reaches well beyond commercial software vendors and encompasses universities, research organisations, and other entities that develop or systematically maintain software made available to third parties.

Although important elements of the CRA's implementation framework, including harmonised European standards and supporting guidance, continue to evolve, the Regulation's principal obligations and implementation timetable are already established. In particular, the incident-reporting requirements commencing in September 2026 apply to products already on the market, making early preparation essential for institutions that develop or govern software within the Regulation's scope.

For higher education institutions, compliance should be regarded not merely as a legal requirement but also as an opportunity to strengthen software governance, improve software supply-chain security, and enhance the long-term resilience and sustainability of research and educational infrastructure. By embedding cybersecurity throughout the software lifecycle and adopting structured vulnerability-management practices, universities can better support secure, trustworthy, and reproducible digital research while meeting the evolving expectations of European cybersecurity regulation.

The Empty Fortress

Securing Montenegro's digital future starts with people, not just laws

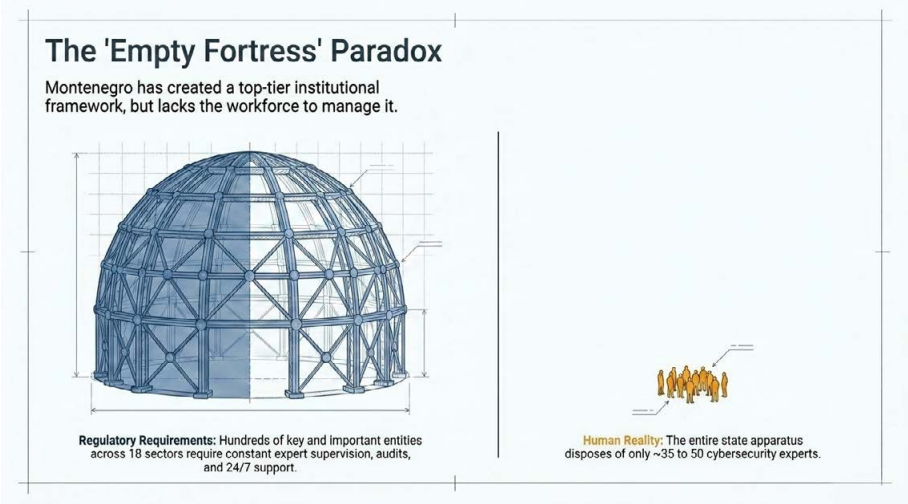
By Jelena Terzić

In 2007, Estonia suffered what is widely regarded as the first state-level cyberattack: a campaign that paralysed government and banking websites for almost three weeks. Estonia's answer was not only better firewalls — it was people: a steady supply of trained professionals built through its schools, universities, and conscript cyber units. Almost two decades later, Montenegro is at a similar point, and facing a similar choice.

The 2022 ransomware attack on Montenegro's government infrastructure made the lesson concrete: laws and firewalls matter far less than the people who run them. When the attack happened, the country had no dedicated cybersecurity agency, no undergraduate degree in the field, and public-sector salaries too low to keep the few specialists trained at home. The 2024 Law on Information Security closed the first gap. The other two are still open.

THE EDUCATION GAP AT A GLANCE

0	undergraduate programmes in cybersecurity
2	master's programmes (combined enrolment under 30 students a year)
0	doctoral programmes or dedicated research groups
~500	qualified IT security professionals missing from the market



Montenegro has built a top-tier institutional framework, but lacks the workforce to run it.

A region-leading law — and no one to run it

Adopted in 2024 and aligned with the EU's NIS2 Directive, Montenegro's Law on Information Security is the most comprehensive cybersecurity legislation in the Western Balkans. It requires every operator of essential services to appoint a Chief Information Security Officer, run ISO 27001-grade risk management, and carry out regular Business Impact Analyses. None of this is trivial. Whether the framework works in practice depends on having enough trained people to implement, audit, and enforce it — and Montenegro does not yet have them. The Agency for Cybersecurity, operational since December 2025, pays on the general civil service scale, well below what private employers or international organisations offer for the same profiles.

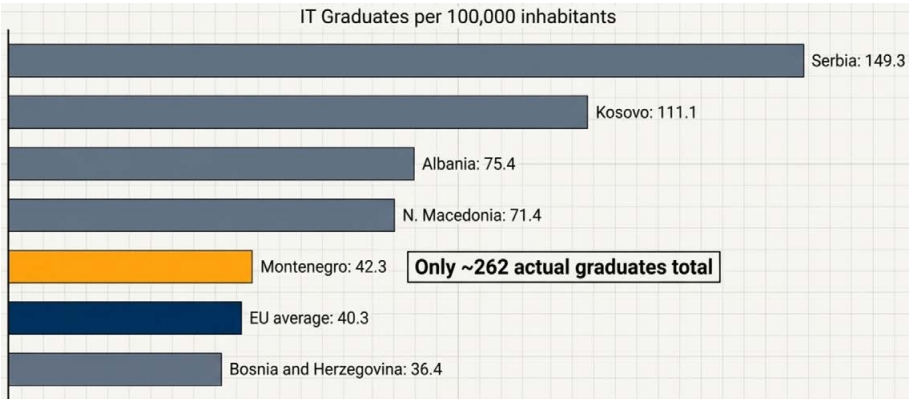
Above the EU average — but the wrong kind of graduate

On paper, Montenegro looks healthy. It produces about 262 IT graduates a year, or 42.3 per 100,000 inhabitants — slightly above the EU average of 40.3. The figure hides a composition problem: almost none of these graduates have any formal training in cybersecurity, and the country's small absolute numbers mean that even a small loss to emigration quickly becomes a critical shortfall.

The shortage is sharpest in Governance, Risk and Compliance — the skills needed to apply risk frameworks, manage audits, and meet legal requirements such as GDPR and the NIS2 Directive. These sit between law, management, and IT, and at present neither the law faculties nor the IT faculties produce graduates who can work in all three.

The invisible brain drain

Remote work has changed the arithmetic. A developer or security analyst no longer has to move abroad to work for a German, Dutch, or American employer; they can stay in Podgorica on a Western European salary. That removes them from the domestic labour supply without ever appearing in emigration statistics — and it hits public institutions hardest. Someone working remotely for a foreign company is not available to staff the Agency, respond to incidents at the national CIRT, or teach part-time at the university. Any strategy aimed only at making physical emigration less convenient misses the point; the fix has to address pay and working conditions directly.

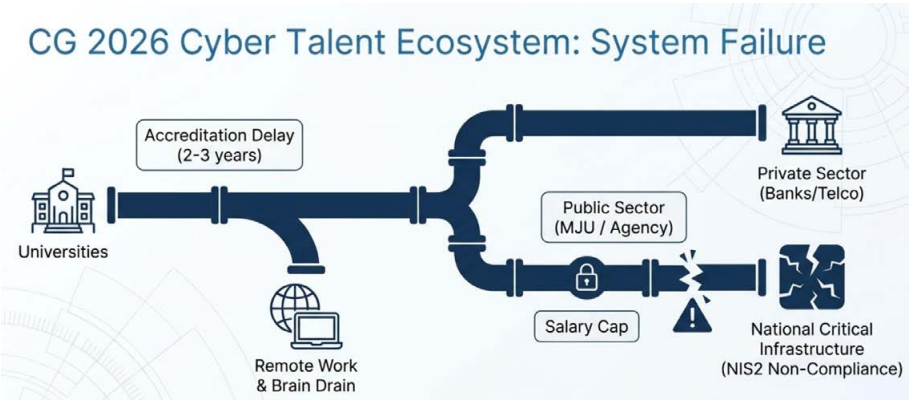


IT graduates per 100,000 inhabitants across the Western Balkans and the EU. Montenegro sits just above the EU average — but its graduates are overwhelmingly generalists.

What needs to happen

Structural problems have structural fixes, and most of these are administrative rather than expensive. Three stand out:

- **Pay for scarcity.** A salary supplement for shortage cybersecurity roles in the Agency and the CIRT, set to close most of the public–private pay gap, is the single highest-impact step — and needs no institutional reorganisation.
- **Teach across faculties.** Required modules on cyber law and information-security risk management at both the law and IT faculties, plus WB3C Cyber Range scenarios built into assessed coursework, would close the GRC gap without creating new degrees.
- **Build for the long term.** A full undergraduate cybersecurity degree, developed through the ULYSSEUS European University alliance, and a doctoral research group to train the next generation of teachers.



The talent pipeline under strain: accreditation delays, salary caps, and remote-work brain drain leave national critical infrastructure exposed.

"If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology."

— Bruce Schneier

Montenegro's first problem is not technology. It is human capital. The NIS2 timeline will not move, the regional WB3C centre is running, and the ULYSSEUS partnership is ready to use. What remains is to treat these as foundations to build on — because in cybersecurity, the strongest fortress is only as good as the people inside it.

This feature draws on the study "Human Capital as the Foundation of Cyber Defence: Closing the Cybersecurity Education and Talent Gap in Montenegro," prepared within the ULYSSEUS Cyber Security Science Shop by the same author.

Protect in Practice: Hands-On Incident Management and Restoration Training in Schwenningen

From 8 to 10 July 2026, representatives of Montenegrin higher education institutions, government bodies and project partners gathered at the Schwenningen Campus of Hochschule Furtwangen for a three-day in-person training dedicated to the Protect (PR) function of the NIST Cybersecurity Framework. Organized by HFU, the programme moved the project from governance documents to the controls, exercises and decisions that keep an institution running when something goes wrong.

The first day established the foundations of access control and data security. After an introduction to the role of the



Protect function in containing incidents, Johannes Lutz (HFU) guided participants through identity management and access control. Role-based access, least privilege and separation of duties were not treated as abstractions: participants configured MFA and access roles for a mock learning management system, then worked through data protections at rest, in transit and in use. The day closed on the data lifecycle, with an exercise in which teams built a backup plan for student records under a fixed budget and had to defend their choices. Deciding between an offline tape in a safe, separate backup credentials, immutability, a quarterly restore drill or a printed runbook with a trained deputy forced a question that rarely gets asked out loud: which of these do we actually have, and when did we last prove it works?

The second day turned to platform and infrastructure resilience. Dr. Jerzy Duda (AGH University of Kraków) opened with configuration management and patching cycles, with participants patching a mock vulnerable application and reviewing platform logs. Niels Schneider (HFU) followed with secure software development in academic settings, where teams hunted for vulnerabilities in sample student code: scored, timed, and set against an AI model working the same snippets. The humans won, but narrowly, and the closing message was the interesting part: the model was fast and confident, missed the quiet flaws, and shipped a fix that could be bypassed.

Prof. Dr. Christoph Reich (HFU) then addressed network segmentation, IDS/IPS, redundancy and disaster recovery, with participants designing a resilience mechanism for a student information system during a power outage. The day ended with a simulated ransomware incident: a phishing mail three weeks earlier, domain admin in the attackers' hands, production encrypted first and the backups hunted next and a draft containment strategy produced under the clock.

The final day connected the technical layers to governance. Dr. Ines Kožuh (University of Maribor and University of Ljubljana) covered cybersecurity awareness and training, distinguishing what general users need from what specialized staff need, and ran a phishing awareness simulation before leading an exercise mapping institutional governance roles to Protect responsibilities. In the capstone workshop, moderated by Branko Marović (University of Belgrade), teams drafted an institutional Protect Action Plan covering IAM, data security, platform security, resilience and awareness, which were peer-reviewed and presented. A closing evaluation session led by Manav Madan and Niels Schneider (HFU) gathered strengths, lessons learned and recommendations for future training activities.

The training forms part of the project's capacity-building activities and directly supports the CSupMNE objective of strengthening cybersecurity preparedness and resilience across Montenegro's higher education sector.

The Chamber of Economy of Montenegro will present two significant initiatives supporting the digital transformation and technological development of Montenegro at **INFOFEST 2026**, one of the region's leading ICT events, taking place **from 27 to 30 September 2026** at the Hotel Avala in Budva, Montenegro.

INFOFEST has, for decades, served as a premier platform for the exchange of knowledge, ideas, and experiences in the field of information and communication technologies. Bringing together representatives of government institutions, academia, the ICT industry, businesses, and international organizations, the event provides a unique opportunity to discuss emerging technological trends, digital innovation, cybersecurity, artificial intelligence, and the future of the digital economy. Under this year's theme, **"Human in the Loop,"** INFOFEST 2026 will focus on the role of human expertise, responsibility, and leadership in an era of rapid advances in artificial intelligence and digital transformation.

During the event, participants will have the opportunity to learn more about the **Montenegrin European Digital Innovation Hub (MontEDIH)**, which provides comprehensive support to small and medium-sized enterprises and public sector organizations in their digital and green transformation journeys. Through a wide range of services, including digital maturity assessments, access to advanced technologies, training, mentoring, and support in accessing finance, MontEDIH helps organizations strengthen their competitiveness and accelerate innovation.

INFOFEST attendees will also be introduced to **CSupMNE – Enhancing Cybersecurity Capacities in Higher Education in Montenegro**, an Erasmus+ project aimed at strengthening cybersecurity education and skills development in Montenegro. The project focuses on modernizing academic curricula, improving institutional capacities, and fostering closer cooperation between academia, industry, and public institutions in the field of cybersecurity.

The promotion of these initiatives at INFOFEST 2026 will provide an excellent opportunity to engage with businesses, ICT professionals, researchers, students, and policymakers, while highlighting the importance of digital innovation, cybersecurity, and international cooperation for the sustainable development of Montenegro's economy.

We invite all interested participants to visit our presentation and discover how MontEDIH and CSupMNE are contributing to the creation of a more digital, innovative, and resilient future.

II
Visit the MontEDIH Info Corner at the Economic Conference Montenegro 2026

The **MontEDIH Info Corner** will be featured at the **Economic Conference Montenegro 2026**, taking place on **30 September – 1 October 2026** at **Hotel Splendid Conference & Spa Resort in Budva, Montenegro**. Recognized as the **largest regional economic gathering**, the Economic Conference Montenegro brings together leading representatives of governments, international organizations, business communities, financial institutions, academia, and other stakeholders to discuss key economic trends, challenges, and opportunities shaping the future of the region.

Within this prestigious platform, participants will have the opportunity to visit the MontEDIH Info Corner, a dedicated space designed to showcase opportunities for digital innovation, business transformation, and technology-driven growth.

The Montenegrin European Digital Innovation Hub (**MontEDIH**) supports small and medium-sized enterprises and public sector organizations in accelerating their digital and green transformation. Through tailored advisory services, digital maturity assessments, access to advanced technologies, skills development, and support in accessing finance, MontEDIH helps organizations strengthen their competitiveness and prepare for the challenges of the digital economy.

Visitors to the Info Corner will be able to learn more about the wide range of services available through MontEDIH, meet project representatives, and explore practical solutions that can support their digital transformation journey.

A particularly important component of MontEDIH is its focus on **cybersecurity**, which has become a critical

prerequisite for successful digitalization and business resilience. As organizations increasingly adopt digital technologies, strengthening cybersecurity capacities and protecting digital assets are essential for ensuring a safe and sustainable digital future.

This topic is also at the core of the **CSupMNE – Enhancing Cybersecurity Capacities in Higher Education in Montenegro** project, implemented under the Erasmus+ Programme. CSupMNE aims to strengthen cybersecurity education, modernize curricula, and develop the skills needed to address emerging cyber threats. By fostering cooperation between academia, businesses, and public institutions, the project contributes to building a more secure digital ecosystem in Montenegro.

The MontEDIH Info Corner will provide a valuable opportunity for conference participants to discover how MontEDIH and CSupMNE are supporting innovation, digital transformation, and cybersecurity readiness, while helping Montenegrin businesses and institutions successfully navigate the digital future.

We invite all participants of the **Economic Conference Montenegro 2026** to visit the MontEDIH Info Corner and explore how digital innovation and cybersecurity can become key drivers of competitiveness, resilience, and sustainable economic growth.

PROJECT HIGHLIGHTS

CSupMNE Partners Strengthen Cybersecurity Capacities through Hands-On Training at Furtwangen University

As part of the Erasmus+ **CSupMNE – Strengthening Cybersecurity in the Academic Sector** project, a three-day professional training programme, **"Protect – Hands-On Incident Management and Restoration,"** was held from **8–10 July 2026** at Hochschule Furtwangen University (HFU), Germany. The training aimed to strengthen the cybersecurity knowledge and practical skills of participants from higher education institutions, with a particular focus on improving institutional protection capabilities, incident management, and recovery processes through the implementation of the **Protect (PR)** function of the NIST Cybersecurity Framework.

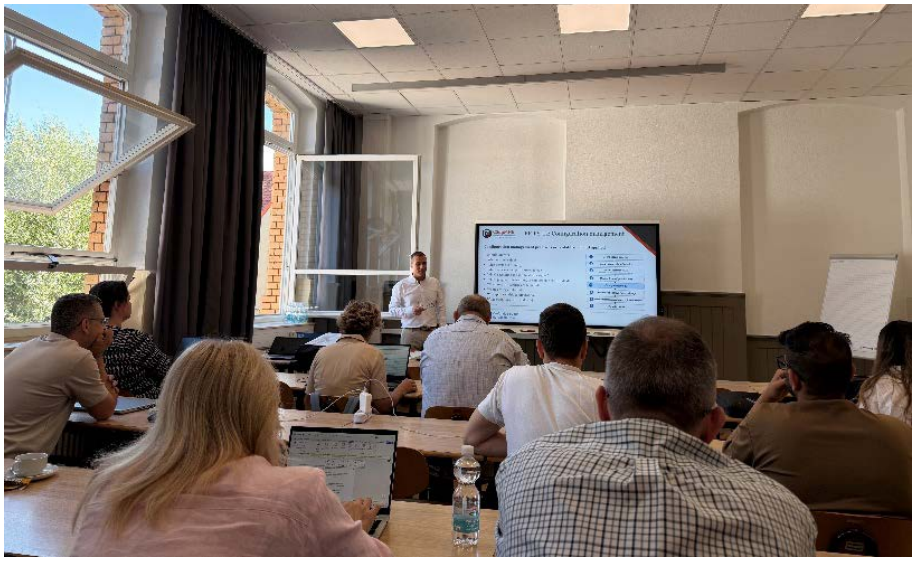
The programme was coordinated by cybersecurity experts from Furtwangen University, including **Prof. Dr. Christoph Reich, Manav Madan, Niels Schneider, and Johannes Lutz**, who combined expert presentations, practical exercises, simulations, and interactive discussions to provide participants with applicable knowledge and hands-on experience.

The first training day focused on the **Protect (PR)** function of the NIST Cybersecurity Framework and its role in preventing and mitigating cybersecurity incidents in higher education institutions. The introductory session, delivered by Manav Madan and Prof. Dr. Christoph Reich, presented the overall structure of the framework and the importance of proactive cybersecurity measures.

Johannes Lutz then introduced participants to the fundamentals of protection services, identity management, authentication mechanisms, and access control, highlighting practical approaches to implementing secure identity and access management practices within academic institutions. The day concluded with a session led by Niels Schneider on **Data Lifecycle and Backup**, covering data retention strategies, backup planning, and recovery testing. Through an interactive browser-based exercise, participants developed backup plans and responded to simulated disaster scenarios, gaining practical experience in protecting institutional data and supporting business continuity.

The second day focused on **Platform and Infrastructure Resilience** and featured contributions from experts

representing leading European higher education institutions. Dr. Jerzy Duda from AGH University of Kraków delivered practical sessions on platform security and adverse scenario simulations, demonstrating approaches to secure platform management, vulnerability mitigation, and effective incident response.



Niels Schneider continued with a session on **Secure Software Development in Higher Education Institutions**, introducing secure coding principles applicable to teaching, student projects, and research environments. Participants analysed security vulnerabilities in sample source code through an interactive browser-based exercise and compared their findings with AI-generated analyses, encouraging critical thinking and discussion about secure software development practices.



The programme also included a session on **Technology Infrastructure Resilience**, delivered by Prof. Dr. Christoph Reich. Participants explored strategies for building resilient institutional infrastructures through network segmentation, redundancy planning, resilience mechanisms, and disaster recovery planning, with an emphasis on practical implementation in higher education environments.

The third training day focused on **Awareness, Integration, and Capstone**, highlighting the importance of integrating cybersecurity into institutional governance while strengthening awareness among staff and students.

Dr. Ines Kožuh from the University of Maribor and the University of Ljubljana led sessions on **Cybersecurity Awareness and Training** and **Integrating PR Domains into Governance**. Participants explored methods for developing cybersecurity awareness programmes and took part in a phishing simulation exercise designed to improve the recognition of cyber threats and the communication of security messages to different target groups. The governance session addressed the integration of identity and access management, data security, platform protection, resilience, and awareness into a coherent institutional cybersecurity strategy through an interactive governance mapping exercise.

The afternoon was dedicated to the **Capstone Workshop – HEI PR Action Plan**, facilitated by Branko Marović from the University of Belgrade. Working collaboratively, participants developed draft Protection and Resilience Action Plans tailored to their institutions, covering key areas such as identity and access management, data protection, platform



security, resilience, and cybersecurity awareness. Peer discussions enabled participants to exchange experiences, review each other's work, and further refine their institutional approaches.

During the final presentations, teams showcased their proposed action plans, identifying implementation priorities, institutional challenges, and opportunities for strengthening cybersecurity resilience. The training concluded with an evaluation session moderated by Manav Madan and Niels Schneider, where participants reflected on the programme's content, delivery methods, and practical relevance, while also providing recommendations for future capacity-building activities.

The training programme was successfully organized by Hochschule Furtwangen University (HFU) at its Schwenningen Campus under the guidance of Prof. Dr. Christoph Reich and coordinated by Manav Madan and Niels Schneider from the IDACUS Institute. Bringing together participants from partner institutions across Montenegro, Germany, Poland, and Slovenia, the event provided an excellent opportunity for international knowledge exchange and collaboration.

By combining expert lectures, practical exercises, simulations, and collaborative workshops, the training significantly strengthened participants' capacities to implement the Protect (PR) function of the NIST Cybersecurity Framework within their institutions. As another important milestone of the CSupMNE project, the event reinforced international cooperation and supported the development of more resilient, secure, and cyber-aware higher education institutions.

The workshop represented another important milestone of the CSupMNE project, reinforcing international collaboration and supporting the development of more resilient, secure, and cyber-aware higher education institutions.

CSupMNE Project Presented at International Days 2026

On **29 July 2026**, **Prof. Dr. Marija Janković** presented the Erasmus+ project **"Strengthening Up Cybersecurity Posture of the Montenegrin Higher Education System (CSupMNE)"** during the **International Days 2026** at the **Powiślańska Academy of Applied Sciences**, Poland.



The presentation introduced the project's overall concept, objectives, work packages, and the key results achieved since the beginning of the project. Participants were informed about the project's mission to strengthen the cybersecurity posture of Montenegro's higher education system by supporting institutional and national reforms, enhancing cybersecurity governance, and improving resilience against cyber threats.

Particular attention was given to the project's progress in modernising higher education through the development of cybersecurity-related study programmes, innovative teaching and learning approaches, digital education standards, and capacity-building activities for academic and administrative staff. The presentation also highlighted activities aimed at increasing cybersecurity awareness across the higher education sector, improving institutional infrastructure through innovative technological solutions, and strengthening operational mechanisms for effective incident response and recovery through the establishment of the Montenegrin Academic CSIRT.

The achievements presented included the implementation of professional training programmes, international study visits, collaborative workshops, and the development of practical resources supporting the adoption of the Cybersecurity Framework within partner institutions. These activities have significantly contributed to strengthening cybersecurity capacities and fostering cooperation among higher education institutions and international project partners.

The presentation provided an excellent opportunity to disseminate the project's achievements, exchange experiences with international colleagues, and promote future cooperation in the field of cybersecurity and digital transformation in higher education.

