HIGH-LEVEL CYBERSECURITY CONFERENCE

CYBERPULSE 2025, 2 July 2025

Conference Summary Report

The High-Level Western Balkans Cybersecurity Conference – CyberPulse 2025: Tracking Progress, Building Resilience, Driving Change was organized by the Regional Cooperation Council (RCC), with the support of the European Commission (EC), and jointly with the Western Balkans Cyber Capacity Center (WB3C), on 2 July 2025 in Podgorica, gathering government representatives, regional and EU institutions, cybersecurity experts, and private sector leaders to address the growing threat of cyberattacks across the region.

Opening the conference, Secretary General of the Regional Cooperation Council, Amer Kapetanović, underlined the urgent need for collective resilience. "Cybersecurity is not just about tech – it's about trust, people, and partnerships. Our greatest firewall will be our shared goals and political will to reach them. The RCC will continue to champion coordinated regional efforts, because cyber threats are borderless, and so must be our response." He cited a significant rise in cyber threats and incidents over the past year: "Cyber incidents in the Western Balkans increased by 40% last year, compromising more than 1.2 million personal data records," stated Kapetanović. RCC SG announced the development of a new regional cybersecurity needs database, a joint effort by RCC, the European Commission, and IISG, which was officially launched at the Donor Coordination Meeting held back-to-back with this conference.

Deputy Prime Minister of Montenegro for Foreign and European Affairs, Filip Ivanović, noted that Montenegro is actively adopting and implementing European cybersecurity standards to bolster resilience against cyber threats. "We are strengthening institutional capacities, integrating with European networks, and developing an economy-level cybersecurity strategy. As a prospective member of the European Union (EU), we will advocate for a European future for the entire Western Balkans, including through a secure, resilient, and smartly connected digital space," he asserted.

Michael Docherty, speaking on behalf of the European Commission Delegation, affirmed the EU's active support for the region through various initiatives, including collaborations with ENISA and the Council of Europe. He emphasized that cybersecurity has been integrated into the reform agendas of the vast majority of Western Balkan economies under the Growth Plan for the region, with the final remaining economy expected to align soon. "Within the European Union framework,

we are achieving significant progress in strengthening cybersecurity across the Western Balkans. It forms a key element of the Growth Plan, including the gradual integration of the region into the EU's single digital market," Docherty noted.

Gilles Schwoerer, Head of Western Balkans Cyber Capacity Centre, underscored that digital transformation brings numerous advantages but simultaneously increases cyber-risk exposure. "Our attack surface is growing exponentially—we need secure digital pathways. Governments in the region are making substantial efforts to enhance cybersecurity resilience, yet cyber threats remain persistent and escalating," he concluded.

High-level panel: Stronger Connectivity, Smarter Security, Resilient Future

The high-level panel, moderated by Danijela Gačević, Head of the Programme Department in RCC, provided a strategic forum for discussing the cybersecurity priorities of the Western Balkans. Designed as a space for informed and forward-looking dialogue, the session brought together highlevel representatives from the three Western Balkan economies, facilitating an exchange of experiences on the economy level, and regional perspectives on pressing cyber challenges.

Deputy Minister of Internal Affairs from Pristina, Bardhyl Dobra, pointed to the lack of human capacities and the need to develop internal resources. The government has made significant strides in strengthening its cybersecurity legal framework; however, it still faces challenges such as limited human resources, competition with the private sector, and reliance on external consultants. "We are grateful for our EU partners and other institutions, but we must build internal capacity within our institutions ourselves. Therefore, we are improving education and training in the public sector," stated Deputy Minister Dobra.

Naim Gjokaj, State Secretary at the Ministry of Public Administration from Podgorica, emphasized that capacity building within institutions is a top priority. The public administration does not face strong private-sector competition in recruiting cybersecurity specialists; nevertheless, intersectoral cooperation remains the focus, and the public sector continues to experience a shortfall of qualified experts. "Building institutional capacity is our main objective. This can only be achieved through cooperation with our partners—NATO and the EU," said Mr Gjokaj.

Deputy Minister for Digital Transformation from Skopje, Radoslav Nastasijevikj Vardjiski, presented the new strategic framework and institutional solutions. Long struggle with outdated legislation and the absence of strategic documents for digitalisation and cybersecurity was one of

the challenges. “To address these challenges, we established the Ministry for Digital Transformation, created a dedicated cybersecurity sector, and adopted a strategy shared with an action plan. The strategy outlines a unified vision with key goals: strengthening institutional capacity and legal frameworks, improving the protection of critical infrastructure, fostering cyber resilience in both public and private sector, and enhancing incident-response coordination,” concluded Deputy Minister Nastasijevikj Vardjiski.

Navigating Cyber Threats in the Western Balkans: The Evolving Role of AI and Emerging Technologies

The panel discussion, moderated by Mirza Jamaković from Prosecutor's Office from Sarajevo, explored the evolving landscape of cyber threats in the Western Balkans, placing particular emphasis on the transformative role of artificial intelligence and emerging technologies in cybersecurity from various sectors. Panelists reflected on organised criminal groups that are increasingly deploying artificial intelligence to produce and distribute illegal content, including child sexual abuse material, phishing campaigns, and online fraud. On the dark web, some groups are even developing their own large language models (LLMs), reflecting a rapid technological evolution within criminal networks.

Emmanuel Kessler from Europol spoke about the use of machine learning for analysing millions of data points – enabling an efficient understanding of how such groups operate. “Europol uses machine learning to analyse millions of data items—images, messages, geolocations—enabling us to efficiently understand how these groups operate. These tools have been instrumental in high-profile cases, helping us comprehend how groups communicate and plan operations, sometimes including threats to life,” explained Kessler from Europol.

Data quality and transparency of AI outcomes are significant challenges across the financial and other sectors. Jelena Zelenović Matone from WomenCyberForce and Women4Cyber discussed the transparency challenges of AI models, especially stressing the need for explainable AI outcomes. “By transparency, I mean explainability. How do you justify why something is classified as ‘true’? What data did you use, and how? Can this be trusted? That is a challenge even within artificial intelligence—can we trust it?” raised Zelenović Matone.

One of the most prevalent forms of cybercrime in the Western Balkans involves cryptocurrency investment scams, often coordinated through regional call centres targeting victims across Europe,

Australia, and Canada. Nenad Bogunović from cybercrime unit from Belgrade presented a forensic tool that detects AI-generated content. Their unit is initiating a project, inspired by Italy's Carabinieri and national police, aimed at detecting such abuses and phishing schemes. "The model works in two ways: one, as a forensic tool for police investigators to detect AI-generated content offline on devices; two, as an online service enabling citizens to check whether they have been victims of internet fraud or unauthorised AI-modified content," explained Bogunović.

Users must exercise caution when submitting confidential data to AI systems. Amar Dedović from Oracle warned against the unsafe use of AI tools in corporate environments, noting that users often, due to haste or lack of awareness, input confidential or sensitive data into generative AI systems that are beyond their control. "Many use ChatGPT to enhance their work or speed up tasks. However, they make a major mistake by uploading confidential documents into ChatGPT, which is not an environment under your control or secure. Those data are sent elsewhere, and if they are confidential, you are creating a significant problem for your company. Many people are doing this, which is why we need regulation to address it," emphasized by Dedović.

Empowering Talent: Skill-Building for the Future in WB

The panel, moderated by Andreja Mihailović from Women4Cyber from Podgorica, provided an engaging and insightful discussion on the importance of advancing skills development in the field of cybersecurity. Special attention was given to the (un)derrepresentation of women and young professionals in the field.

The cybersecurity sector still harbors considerable untapped potential, especially in relation to women's participation. While they constitute more than half the population, their presence in ICT remains below 20%. However, international collaboration demonstrates that with a strategic approach, change is achievable. "A prime example of international cooperation boosting female expertise and participation is the UN Cybersecurity Working Group. When we began in 2019, women represented 30%. Last year, that number rose to 52%. In just five years, we increased female participation by 20%," stated Tamara Tafra, Deputy Minister of Foreign and European Affairs from Zagreb.

Igli Tafa, Director of the Cybersecurity Agency from Tirana, discussed the need for educational reform. Sustainable regional cooperation and systematic solutions beginning at the primary school level are among the strategies that could be used to address workforce shortages. "Capacity building is not just infrastructure—it does not yield sustainability on its own. We must reinvent curricula from primary school through university to build a sustainable system and a secure digital

environment. Second, cooperation. Unfortunately, within the Western Balkans, we have not made sufficient progress in collaboration," highlighted Tafa.

Andi Dobrushi from the Open Society Foundation stressed the importance of redirecting young people from the grey digital zone to formal sectors. Concerns have emerged regarding increased cryptocurrency mining among youth and potential money laundering. Therefore, Dobrushi suggests redirecting this human capital—young people working in the grey or even criminal digital zone—into legitimate digital sectors to help mitigate regional capacity shortages. "That has become a priority for us in employment policy. We are seriously examining how to redirect this emerging workforce towards positive digital avenues. We hope this will help alleviate the capacity deficit," explained Dobrushi.

To achieve real impact, institutions must channel and coordinate capacity wisely. Cybersecurity is inherently multidisciplinary and cannot be managed by one individual alone. Fabio di Franco from ENISA pointed to the need for specialisation and sectoral division of responsibilities within large systems. Large organisations and public administration must establish specialised units or inter-agency cooperation. "We're talking about different domains—one person cannot cover everything. That may be feasible in small organisations, but in larger ones or government bodies you need a structure with distinct sectors or a department that renders services to others. It's like doctors—you don't go to one for every problem," concluded di Franco.

Integrating Experience and Strategy: A Multisector Dialogue on SOC Advancement

The panel, moderated by Vanja Madžgalj from the Western Balkans Cyber Capacity Centre, from Podgorica, provided a valuable platform for exchanging knowledge and practical experiences on the systematic development of Security Operations Centres (SOCs). The discussion highlighted diverse practices and institutional models for SOC establishment and operation, presenting examples of good practice from both private and public sector.

Franc Zyliftari, Head of the Incident Response Team from Tirana, shared experiences in developing a strategy on economy level following the 2022 cyberattack. That cyberattack served as a wake-up call, prompting the economy to accelerate cybersecurity capacity development and strengthen preventive measures. "The key skill lies in detecting suspicious activity before it escalates into a full-blown incident. Facing such threat actors compelled us to build capacity, gain experience, and implement best practices in cybersecurity—such as zero trust and defense-in-depth—which today, aided by AI and machine learning, help keep our cyberspace safe and secure," highlighted Zyliftari.

Philippe Gillet, from Gatewatcher from Paris, noted essential differences in threat-intelligence usage between the public and private sectors. “Threat intelligence is more readily adopted in the private sector because companies are inclined towards open communication and data sharing. Public institutions, on the other hand, often withhold information, making trust-building harder. In private sector you earn trust by delivering software—clients have no choice but to trust. In the public sector it’s more challenging, because they don’t share all their data. For threat intel to be effective, it must be personalised to the client’s context,” Gillet explained.

Alignment of policy, legal regulation, and inter-sectoral cooperation is central to effective cybersecurity, underlined Aleksandar Acev from Cyber Balkans from Skopje. He pointed to a new law that designates the Ministry for Digital Transformation as the central authority setting security standards. “But the law also allows for so-called sectorial competent authorities—for example, in banking. Every economy has a central bank that long ago established policies, procedures, and a minimum set of controls that banks must follow—and all banks comply,” he added.

Sectors United Against Cyber Threats: Building Bridges Across Sectors

The panel, moderated by Milan Sekuloski from e-Governance Academy from Tallinn, explored the complementary roles of public and private sector, academia and civil society in advancing cybersecurity across the Western Balkans. The discussion offered a multi-stakeholder perspective on how these actors contribute to building a resilient cyber ecosystem, while also addressing the critical support needs of the public sector.

Lulezon Jagxhiu, from the Prime Minister’s Cabinet from Pristina, stressed that cybersecurity must be a shared responsibility. Their experience is that initiatives related to critical infrastructure which regularly bring together all relevant actors to exchange information and coordinate measures provide another example of the importance of inter-sector collaboration. “In traditional security, there’s always the perception that government has a monopoly. In cybersecurity, we must change that mindset—it is an ecosystem of shared responsibility. All actors must not act in isolation, but together—sharing information, dialoguing, and collaborating on policies,” emphasized Jagxhiu.

Non-governmental organisations frequently perform highly sensitive and important work and therefore require adequate protection. Focused on niche areas of expertise, they design projects and initiatives with significant societal impact. Predrag Puharić, from Cybersecurity Centre of Excellence from Sarajevo, highlighted the need for supporting the civil sector. Recognising this, the Center understood the necessity of bolstering civil society’s defense of digital assets. “We thought we needed to protect them—actually to help them protect themselves—by promoting

cyber hygiene. Through work with civil society, we developed targeted tools, guidelines, documents, and training dealing with issues that were critical and urgent for them," noted Puharić.

Ivona Dabetić from the NGO Secure from Podgorica emphasized the importance of cooperation among the private, public, and academic sectors, presenting the vulnerable position of small and medium-sized enterprises in the cybersecurity landscape. Supporting businesses in understanding risk and developing fundamental security practices is essential to their resilience and sustainability in today's digital environment. "Of course, the idea is not for everyone to do everything, but for each sector to contribute its strength: private sector with technical expertise and innovation, public sector with systemic support, policies, frameworks and cooperation, academia with research, analysis and education, and NGOs as bridges to communities—including underserved populations, raising awareness and democratising access to knowledge," emphasized Dabetić.

Cybersecurity has also emerged as an economic priority. Roy Yarom from the EBRD presented the Bank's approach, which links investment with technical support and the strengthening of local capacities. While digitalisation is essential for improving competitiveness and inclusion, it also brings serious security risks, especially in sectors such as energy, telecommunications, and finance. "When we invest in projects like new power plants, cyber threats are very real and can threaten the long-term viability of these projects. Therefore, beyond financing, we provide technical support, training, and risk assessments to ensure their protection," stated Yarom.

The conference concluded that cybersecurity is no longer merely a technical or IT matter, but a strategic priority requiring long-term cooperation, education, a robust legislative framework, and investment in human resources. Regional resilience to cyber threats can only be achieved through a coordinated approach and active information exchange among all relevant stakeholders.