

# Cyber Capacity Building Workshop: Western Balkans

**Date:** 19 – 20 May 2025

**Location:** Western Balkans Cyber Capacity Center, Podgorica, Montenegro

## Workshop description

The global cybersecurity landscape is evolving at an unprecedented pace, driven by rapid digitalization, increasingly sophisticated cyber threats, and growing dependence on critical digital infrastructure. According to the [Global Cybersecurity Outlook 2025](#), ransomware remains the top cyber risk for organizations worldwide, with 45% of respondents ranking it as their primary concern. Additionally, 66% of organizations anticipate that artificial intelligence (AI) will have the most significant impact on cybersecurity in the coming year.

In the Western Balkans, the threat landscape is also intensifying. [Research](#) indicates that in 2023, cyber incidents in the region increased by 40%, while ransomware attacks surged by 200% between 2022 and 2024. As cyber threats grow more sophisticated and persistent, governments and businesses in the region must strengthen cybersecurity capabilities, enhance cross-border collaboration, and invest in workforce development to effectively mitigate risks.

To tackle these challenges, the Western Balkans Cyber Capacity Center (WB3C) and the World Economic Forum (WEF) will host a Cyber Capacity Building Workshop on May 19-20 in Podgorica, Montenegro. This two-day workshop will bring together key stakeholders, including government officials, industry leaders, academia, and law enforcement, to discuss:

- Approaches on how to address the cyber talent shortage in the region (Stream 1).
- Collaborative strategies to out-manoeuvre cybercriminals in the Western Balkans (Stream 2).

*The working language of the workshop is English.*

## Workshop agenda

Day 1 19 May 2025	
Time	Activity
9:30 – 10:00	Welcome coffee
10:00 – 10:15	Opening remarks: Gilles Schwoerer, WB3C Programme Director
10:15 – 10:30	Keynote by Mr Maraš Dukaj, Minister of Public Administration, Government of Montenegro
10:30 – 11:15	Opening panel: Cybersecurity in the Western Balkans: Bridging global practices with local needs  Contributors: <ul style="list-style-type: none"><li>• Dušan Polović, General Director at the Directorate for Infrastructure, Information Security, Digitalization and E-services the Ministry of Public Administration (Montenegro)</li><li>• Ivan Bošković, President of e-Commerce Association of Montenegro (Montenegro)</li><li>• Jelena Zelenović Matone, Chief Information Security Office, European Investment Bank (Luxembourg)</li></ul>

	<ul style="list-style-type: none"> <li>• Rob Rashotte, Vice-President, Global Training and Technical Field Enablement, Fortinet (Canada)</li> <li>• Samuel Hassine, Chief Executive Officer, Filigran (France)</li> </ul> <p>Facilitator: Nataša Perućica, Lead, Capacity Building, Centre for Cybersecurity, World Economic Forum (Switzerland)</p>	
	<b>Stream 1: Addressing the Cyber Talent Shortage in the Western Balkans</b>	<b>Stream 2: Securing the Digital Realm: Collaborative Strategies to Out-manoeuvre Cybercriminals in the Western Balkans</b>
11:15 – 11:30	Coffee break	
11:30 – 11:45	<p>Workshop introduction and aims</p> <p>Contributors:</p> <ul style="list-style-type: none"> <li>• Nataša Perućica, Lead, Capacity Building, Centre for Cybersecurity, World Economic Forum (Switzerland)</li> </ul>	<p>Workshop introduction and aims</p> <p>Contributors:</p> <ul style="list-style-type: none"> <li>• Seán Doyle, Lead, Cybercrime Atlas Initiative, Centre for Cybersecurity, World Economic Forum (Switzerland)</li> </ul>
11:45 – 13:15	<p>Attracting and recruiting the right talent into cybersecurity</p> <p>Contributors:</p> <ul style="list-style-type: none"> <li>• Denise Cassidy, EMEA Security HR Lead, Accenture (Ireland)</li> </ul> <p>Discussion questions:</p> <ul style="list-style-type: none"> <li>• What are the main causes of the cybersecurity talent shortage in your region?</li> <li>• What challenges do organizations face when attracting cyber talent in the Western Balkans?</li> <li>• What cybersecurity skills and competencies are most in-demand in your region?</li> <li>• What incentives can organizations offer to attract cybersecurity professionals?</li> </ul>	<p>The evolving cybercrime landscape</p> <p>Contributors:</p> <ul style="list-style-type: none"> <li>• Céline Louyat, Inspector, Public Finance, AGRASC (France)</li> <li>• Jelena Zelenović Matone, Chief Information Security Office, European Investment Bank (Luxembourg)</li> <li>• Livia Tirbina, Cyber Threat Intelligence Analyst, Sekoia.io (France)</li> <li>• Paul-Alexandre Gillot, J-CAT Coordinator, Europol, EC3 (France)</li> <li>• Samuel Hassine, Chief Executive Officer, Filigran (France)</li> <li>• Seán Doyle, Lead, Cybercrime Atlas Initiative, Centre for Cybersecurity, World Economic Forum (Switzerland)</li> </ul> <p>Discussion questions:</p> <ul style="list-style-type: none"> <li>• What are the primary cybercrime risks in your country/region?</li> <li>• What are the challenges you face in responding to cybercrime?</li> </ul>
13:15 – 14:15	Lunch	

14:15 – 16:15	<p>Educating and training cybersecurity professionals</p> <p>Contributors:</p> <ul style="list-style-type: none"> <li>Dana Berman, Manager, Strategic Business Development &amp; Marketing - Cybersecurity Services, Check Point Software Technologies (Israel)</li> <li>Reza Elgalai, Université Technologique de Troyes (France)</li> <li>Rob Rashotte, Vice-President, Global Training and Technical Field Enablement, Fortinet (Canada)</li> </ul> <p>Discussion questions:</p> <ul style="list-style-type: none"> <li>What are the key gaps in current cybersecurity education and training programs?</li> <li>How can educational curricula on cybersecurity be standardized across the region?</li> <li>What role should public-private partnerships play in the region in training cybersecurity professionals?</li> </ul>	<p>Anatomy of a cybercrime</p> <p>Contributors:</p> <ul style="list-style-type: none"> <li>Alex Wloch, Senior Analyst, Active Threat Monitoring, Standard Chartered Bank (United Kingdom)</li> <li>Samuel Hassine, Chief Executive Officer, Filigran (France)</li> <li>Sean Doyle, Lead, Cybercrime Atlas Initiative, World Economic Forum (Switzerland)</li> </ul> <p>Discussion questions:</p> <ul style="list-style-type: none"> <li>What area would you/your organisation prioritise for collaboration to counter cybercrime, and why?</li> <li>How can we encourage private and public sector organisations in the region to collaborate?</li> <li>What are some examples where collaboration has helped or could help? How?</li> <li>What specific actions or resources are needed to build stronger operational collaboration?</li> </ul>
16:15 – 16:30	Coffee break	
16:30 – 18:00	<p>Public sector solutions to bridge the cyber talent gap</p> <p>Contributors:</p> <ul style="list-style-type: none"> <li>Abdullah Albaiz, General Manager for Human Capital Development, National Cybersecurity Authority of Saudi Arabia (Saudi Arabia)</li> <li>Grace Boyling, Senior Policy Advisor on International Cyber Skills, Department for Science, Innovation and Technology (United Kingdom)</li> <li>Mark Mannheim, Programme Manager, Cybersecurity and Digital Identity Directorate, Department for Science, Innovation and Technology (United Kingdom)</li> </ul> <p>Discussion questions:</p> <ul style="list-style-type: none"> <li>Could resource limitations or competing priorities affect cybersecurity talent initiatives?</li> </ul>	<p>Key elements of a successful collaboration to combat cybercrime</p> <p>Contributors:</p> <ul style="list-style-type: none"> <li>Paul-Alexandre Gillot, J-CAT Coordinator, Europol, EC3 (France)</li> <li>Seán Doyle, Lead, Cybercrime Atlas Initiative, Centre for Cybersecurity, World Economic Forum (Switzerland)</li> </ul> <p>Discussion questions:</p> <ul style="list-style-type: none"> <li>How might we incentivize partnerships across borders and with the private sector?</li> <li>What resources are needed to collaborate and how might we develop or access them?</li> <li>How might the public and private sectors share important data and insights more effectively over time?</li> <li>How can we coordinate investigations that include both public and private sector partners?</li> </ul>

	<ul style="list-style-type: none"> <li>What are your country's strengths in cyber skills collaboration across government, academia and industry?</li> <li>Are your current government policies sufficient to bridge the cybersecurity talent gap? If not, why?</li> </ul>	
Day 2		
20 May 2025		
8:30 – 9:00	Welcome coffee	
09:00 – 10:30	<p>Retaining cybersecurity professionals</p> <p>Contributors:</p> <ul style="list-style-type: none"> <li>Jakub Olszewski, Head of Skills Academies, Standard Chartered Bank (United Kingdom)</li> </ul> <p>Discussion questions:</p> <ul style="list-style-type: none"> <li>What challenges do organizations in the Western Balkans have in retaining cyber talent?</li> <li>How can organizations keep cybersecurity professionals engaged and motivated?</li> <li>What do you think are the methods of retaining cyber talent?</li> </ul>	<p>Leveraging public-private collaboration to combat cybercrime</p> <p>Contributors:</p> <ul style="list-style-type: none"> <li>Seán Doyle, Lead, Cybercrime Atlas Initiative, Centre for Cybersecurity, World Economic Forum (Switzerland)</li> </ul>
10:30 – 10:45	Coffee break	
10:45 – 11:30	Setting the Strategic Cybersecurity Talent Framework in motion	How to accelerate operational collaboration?
11:30 – 12:30	Closing session: Key takeaways and highlights	
12:45 – 14:00	Lunch	