# FROM DIALOGUE TO ACTION: Working Group Outcomes and Recommendations from the 9th Regional Security Coordination Conference 2024

RegionalCooperationCouncil

Funded by
the European Union

Ministry of Foreign Affairs
and International Cooperation

**Title:**
**From Dialogue to Action: Working Group Outcomes and Recommendations from the 9th Regional (Jumbo) Security Coordination Conference 2024**

**Publisher:**
Regional Cooperation Council
Trg Bosne i Hercegovine 1/V,
71000 Sarajevo Bosnia and Herzegovina
Tel: +387 33 561 700; Fax: +387 33 561 701
rcc@rcc.int
www.rcc.int

**For publisher:**
Regional Cooperation Council

**Authors:**
Mirsad Buzar (Ph.D.), Trpe Stojanovski (Ph.D.), Metodi Hadji-Janev (Ph.D.)

**Editor:**
Aner Zuković (M.A.), RCC

**Design:**
Samir Dedić

**December 2024**

*Disclaimer: Responsibility for the content, views, interpretations and conditions expressed herein rests solely with the author(s) and can in no way be taken to reflect the views of the Regional Cooperation Council (RCC) or of its participants, partners, donors or the European Union.*

Ministry of Foreign Affairs
and International Cooperation

*Regional Security Coordination Conference project was financed with the contribution of the Ministry of Foreign Affairs and International Cooperation of the Republic of Italy. The content of this document represents the views of its authors and in no way represents the position of the Ministry of Foreign Affairs and International Cooperation of Italy.*

Funded by
the European Union

*The production of this publication is financially supported by the European Union.*

# CONTENTS

# 1. INTRODUCTION

The Western Balkans, aspiring to EU integration, continue to grapple with a multifaceted security landscape, marked by ethnic and political tensions and external influences. These challenges are compounded by established and emerging threats such as cybersecurity threats, transnational organised crime, corruption and extremism and terrorism.

The current geopolitical context is also characterised by heightened tensions between global powers, influencing regional stability. The region faces the impact of these tensions at the crossroads of East and West. The Russian invasion of Ukraine has also underscored the importance of regional resilience and the necessity for robust security frameworks. Fake news and disinformation continue to be a great concern, while cyber-attacks are a major threat to regional security and stability. The current circumstances dictate the importance of sustaining the highest level of engagement in regional cooperation, unleashing the joint potential and working together as real partners in addressing the challenges and shaping our joint future. In a world where size and weight matters and none of our economies can lead this fight alone, regional security cooperation is in the WB's strategic and security interest.

The EU and the Western Balkans share security challenges and are addressing them together. They cooperate on a wide range of security issues such as fighting organised crime, tackling hybrid and cyber threats, countering small arms trafficking and strengthening counter-terrorism, etc. With both sides being fully committed to the EU integration of the region, the continuation of tackling the overall spectrum of threats and challenges jointly remains a strategic objective.

The region's strategic importance for the European security cannot be overlooked, particularly due to its being surrounded by EU Member States and its economies perspective to become fully-fledged members of the EU, including its security architecture. Cooperation and dialogue in the area of Common Security and Defence Policy as well as their deepening and expanding are already a strategic priority for both.

Against this backdrop, the 9th Annual Regional Security Coordination Conference (Jumbo) appears to be an important platform for addressing the region's most pressing security challenges.

Held on 7–8 November 2024 in Sarajevo under the theme Working Together in Times of Global Uncertainties, the conference brought together over 150 officials, experts in politics, security, diplomacy, and international stakeholders. Hosted by the Regional Cooperation Council (RCC) with financial support by the Ministry of Foreign Affairs and International Cooperation of Italy and a strong backing of the Italian Ministry of Interior, the event promoted collaboration, shared expertise, and developed solutions to safeguard the region's stability.

The conference featured a dynamic programme, beginning with opening remarks delivered by Majlinda Bregu, RCC Secretary General, alongside Edin Dilberović, Acting Secretary at the Ministry of Foreign Affairs of Bosnia and Herzegovina; Luigi Soreca, Head of the Delegation of the European Union to Bosnia and Herzegovina; Thomas Botzios, Director for the Adriatic and Balkans at the Ministry of Foreign Affairs and

MINISTERO DELL'INTERNO
DIPARTIMENTO DELLA PUBBLICA SICUREZZA
9th Annual Regional Security Coordination Conference in the Western Balkans

*RCC Secretary General Majlinda Bregu opening the 9th Regional Security Coordination Conference dubbed "Working Together in Times of Global Uncertainties", on 7 November 2024 in Sarajevo (Photo: RCC/Jasmin Sakovic)*

International Cooperation of Italy; and Stefano Gambacurta, Deputy Director General of Public Security at the Italian Ministry of Interior. Prefetto Gambacurta emphasized the shared commitment to creating a safer environment for both the region and the EU while also enhancing societal resilience.

"Our region is affected by nearly every global challenge, and our security landscape is rapidly evolving. Migration is not just a flow of people; it's a security issue. Brain-drain is now a security threat, not just an economic issue. We face climate change and natural disasters, and due to ever-growing menace of cyber threats, we are permanently under attack, where our personal lives can be easily violated and invaded at any moment. We are in dire need of prioritising awareness, knowledge, and skills, aligning legislation with the EU, and joining forces with the EU on several fronts. As the EU is embarking on building a 'real European Defence Union' and to 'create a true Single Market for Defence', the Western Balkans has to be kept within arm's length while monitoring the security challenges. Thus, our commitment to building a resilient, adaptive, and forward-looking security framework is a must. By working together on cybersecurity, firearms control, climate resilience, and more, we are enhancing security for the Western Balkans and all of Europe," said Majlinda Bregu, RCC Secretary General, in her opening remarks.

Keynote speaker Federica Mogherini, Rector of the College of Europe and former EU High Representative for Foreign Affairs and Security Policy, reflected on the EU's strategic priorities in the Western Balkans. She emphasized that the region's integration is not merely about "enlargement" but "filling a gap" to complete the European circle, reinforcing shared values and unity. Drawing on her tenure as the EU's High Representative, she highlighted the continuity of policies towards the Western Balkans, noting that even changes in U.S. administrations, including the election of President Trump, did not alter strategic commitments to the region. Mogherini underscored the region's inherent European identity, stressing the importance of fully integrating it into the European framework.

The programme also included a panel discussion moderated by Dr. Leon Hartwell, a Visiting Fellow at the European Leadership Network (ELN), exploring public security perceptions based on insights from SecuriMeter 2024. The panel featured distinguished experts and practitioners who provided perspectives on aligning security policies with public concerns.

Three thematic working groups (WGs) followed, tackling relevant topics, including border/boundary security and migration management, organised crime and corruption, and cyber threats. These discussions culminated in presentations of their findings, which form the core focus of this report. The insights and recommendations generated by these working groups aim to provide solutions for addressing the region's most pressing security challenges while aligning with broader European and global security frameworks. Each WG, led by a distinguished expert, produced significant recommendations.

The first working group session, Strengthening Border Security and Managing Migration, was led by Mr. Mirsad Buzar, PhD, Legal Advisor and Coordinator of the ECT team at GIZ Bosnia and Herzegovina, and former Deputy Director of the Service for Foreigners' Affairs of Bosnia and Herzegovina.

The second working group session, Countering Organised Crime and Corruption, was led by Mr. Trpe Stojanovski, PhD, Professor at the Faculty of Security, St. Kliment Ohridski University, and Senior Advisor at the Global Initiative against Transnational Organized Crime.

The third working group session, Countering Cyber Threats in the Western Balkans, was led by Mr. Metodi Hadji-Janev, PhD, an Associate Law Professor at the General Mihailo Apostolski Military Academy in Skopje.

As the event concluded, one message was clear: collective action is essential to overcoming shared challenges. The RCC is committed to translating the working groups' recommendations into this comprehensive report to guide policy decisions, promote transparency, and stimulate continued dialogue amongst stakeholders.

The 9th Jumbo Conference reaffirmed its position as a cornerstone event for regional security cooperation, setting the stage for sustained progress and deeper collaboration in the years ahead.

# 2. WORKING GROUP SUMMARIES

MINISTERO
DELL'INTERNO
DIPARTIMENTO DELLA PUBBLICA SICUREZZA
RegionalCooperationCouncil
Ministry of Foreign Affairs and International Cooperation
9th Annual Regional Security Coordination Conference in the Western Balkans
Working Together in Times of Global Uncertainties
7-8 November, Sarajevo

**The first working group session, Strengthening Border Security and Managing Migration**, emphasized the critical importance of border/boundary security and migration management for the stability of the Western Balkans (WB) and EU security. Key challenges include irregular migration, organised crime, and limited resources, with smuggling networks exploiting weak border/boundary controls. Migrant smuggling, often involving armed groups, poses significant risks to law enforcement and local communities. Inconsistent visa policies, inadequate readmission agreements, and fragmented data-sharing frameworks further exacerbate these issues. The Working Group recommended harmonising WB visa policies with EU standards, enhancing integrated border/boundary management systems, and fostering regional cooperation through joint investigations and information sharing. Capacity-building measures, such as advanced biometric systems and specialised training for law enforcement, were highlighted. Addressing corruption at border/boundary points is vital to strengthening security. The report underscores the need for a comprehensive approach that aligns regional policies with EU standards to manage migration effectively while safeguarding human rights.

**The second working group session focused on Countering Organised Crime and Corruption** and highlighted these issues as major threats to the stability and governance of the Western Balkans. Criminal networks exploit institutional weaknesses, economic vulnerabilities, and cross-border/boundary complexities to engage in drug trafficking, human trafficking and money laundering. Corruption within the law enforcement and judicial systems undermines efforts to combat these crimes, leading to public distrust. Key recommendations include establishing independent anti-corruption bodies, harmonising oversight mechanisms, and streamlining asset confiscation processes. Strengthening regional cooperation via joint task forces, intelligence-sharing platforms like Europol's SIENA, and cross-border/boundary operations is essential. Investments in digital forensics tools, financial monitoring systems, and capacity-building programmes were also emphasised. Promoting gender diversity in law enforcement is highlighted as a strategic advantage. The workshop calls for sustained political commitment to addressing systemic corruption while fostering regional solidarity against organised crime through enhanced governance frameworks.

At the 9th Regional Security Coordination Conference, **the Working Group on Cybersecurity** addressed escalating cyber threats in the Western Balkans due to limited resources, fragmented governance frameworks, and increasing sophistication of attacks like ransomware and phishing. Critical infrastructure sectors such as finance and telecommunications are particularly vulnerable. Geopolitical tensions further complicate cybersecurity efforts as some foreign state-sponsored entities exploit digital vulnerabilities. Recommendations include establishing a regional Cyber Threat Intelligence Network for real-time threat sharing and aligning cybersecurity frameworks with EU standards. Investments in advanced technologies like AI-driven threat detection and quantum-resistant encryption are essential to counter emerging risks. Public-private partnerships (PPPs) should foster innovation in cybersecurity defence. Enhanced coordination amongst economy-level Computer Security Incident Response Teams (CSIRTs) is needed for effective incident response. The report highlights the importance of a unified regional approach to mitigate hybrid threats, combining cyberattacks with disinformation campaigns while promoting workforce development in cybersecurity skills.

# 2.1 WORKING GROUP 1 REPORT: STRENGTHENING BORDER SECURITY AND MANAGING MIGRATION

**Author: Mirsad Buzar, PhD,**

**Legal Advisor, GIZ Bosnia and Herzegovina**

## 2.1.1 Introduction

The Regional Cooperation Council (RCC), in cooperation with the Ministry of Interior and the Ministry of Foreign Affairs and International Cooperation of the Republic of Italy, organised the 9th Regional Security Coordination Conference in the Western Balkans *Working Together in Times of Global Uncertainties*, which was held in Sarajevo on 7-8 November 2024. The primary goal of the conference was to strengthen regional cooperation and resilience by fostering a collaborative approach to security challenges. The conference served for greater awareness on aligning regional security mechanisms with the European Union (EU) standards, ensuring a stable and secure future for the Western Balkans (WB). Additionally, it aimed to provide a platform for regional stakeholders to update each other on ongoing activities and needs.

The concept of this year's conference was to employ an approach that includes the work and discussions of working groups on all major security issues. Considering that effective border/boundary security and migration management are essential for regional stability and European security, the Working Group (WG) on Border Security and Migration Management also met. Border/boundary security issues are high on the European Union's security agenda. The problem of cross-border/boundary crime is becoming more pronounced, in particular drug, arms, and human trafficking, and tobacco, and migrant smuggling and, while Organised Crime Groups (OCGs) are growing in strength. In response to the migrant crisis and the movement of irregular migrants towards EU member states, there is a need for more efficient border/boundary protection and migration management. Political instability, insecurity, war, poverty and climate change continue to be major drivers of migration, and OCGs operate in areas that pose serious security challenges and threats. The WG addressed the challenges of border/boundary management and migration flows in the WB, and discussed the importance of managing migration flows and securing borders/boundary, as well as the role of the WB in these efforts.

In total, eighteen high-level representatives of the relevant authorities of the WB, EU, diplomats, security professionals, representatives of regional initiatives such are MARRI and IISG, regional projects like EU4FAST, international organisations and academia took part in the work of the WG. As part of the preparations for this year's conference and the organisation and work of the WG, specific questions were prepared by organisers to guide the discussion. The members of WG openly discussed the challenges, problems and weaknesses in their work, identified the gaps, shared their experiences and presented best practices on the basis of which a number of recommendations were made.

## 2.1.2 Overview of the Working Group Discussion

The discussion highlighted that border/boundary security and migration management are very important security issues today, that they are interrelated, and that strengthening them requires a comprehensive approach based on clear policies, risk assessments and plans. This issue is very complex and should be viewed through the prism of legal and irregular migration, integrated border/boundary management issues, law enforcement capacity, readiness, access and performance, visa policy, return and readmission policy, foreign employment policy, as well as corruption issues.

First and foremost, the WB has an important geo-strategic position and is an area of interest and political pressure for major world powers. The area is also known for drug, arms and migrant smuggling routes and other forms of transnational crime, and if relevant authorities in the WB are not able to effectively counter all forms of security threats, this may affect the security of the WB and the EU. What the WB economies have in common is the fact that all of them are on the road to EU accession, but at different stages of negotiations and fulfilment of requirements. It is also a fact that migrants see the WB economies only as transit route to the EU member states, and in order to move and avoid sanctions for illegal entry, they mainly seek international protection - asylum. It is important to emphasize that the WB economies have different security systems, agencies and institutions with different competencies, that each economy creates its own policies and strategies and has different legislation, and that not all economies are at the same level in terms of capacities and degree of their readiness to maintain border/boundary security as well as migration management. One of the main problems and challenges faced by the competent authorities is the lack of sufficient number of police officers working at border/boundary crossings and in border/boundary protection, as well as the lack of specialised equipment for border/boundary surveillance and control, preventing attempts of illegal border/boundary crossings and the use of forged documents.

The latest different dynamics of irregular migration on the WB route, change in the structure of migrants from refugees to economic migrants and the movement of vulnerable categories, women and children, including the change in the routes of movement of irregular migrants in the WB, have posed various challenges to the competent authorities. Establishment and management of reception centres for migrants and work with vulnerable categories of migrants in which international organisations and NGOs play an important role, as well as the placement of potential victims of trafficking in safe houses and further support were also significant challenges. Although there is a need to review trends across the WB, statistical indicators are still not available in one place, although there has been some initiative by the Migration, Asylum, Refugees Regional Initiative (MARRI) to unify and present data.

9th Annual Regional Security Coordination Conference in the Western Balkans
Working Together in Times of Global Uncertainties
7-8 November, Sarajevo

*Mr. Edin Dilberović, Acting Secretary, Ministry of Foreign Affairs, Bosnia and Herzegovina at the 9th Regional Security Coordination Conference dubbed "Working Together in Times of Global Uncertainties," on 7 November 2024 in Sarajevo (Photo: RCC/Jasmin Sakovic)*

It was also emphasized that not all economies in the WB face the same challenges, particularly in terms of the volume of irregular migration and the length of stay of irregular migrants, as well as the activities of organised criminal smuggling groups. Migrant smuggling and human trafficking were identified as a serious security challenge in the WB, with a direct impact on border/boundaries security and migration management. Migrant smuggling on the WB route has been almost entirely taken over by migrant smuggling groups, which have recently become well-armed. Questions remain about where these groups obtain weapons, whether they move them across border/boundary, and how to counter them effectively. The rivalry between the smuggling groups manifests itself in their mutual confrontations using firearms, resulting in killings and fear of the local population in these areas, which sometimes manifests itself in protests and leads to a serious security violation. These groups use a new modus operandi, kidnapping migrants, mistreating them in a very cruel way and demanding ransom from their families for their release, with Afghan smuggling groups being particularly prominent. There have also been documented cases of smuggling groups using violence against police officers trying to prevent the smuggling of migrants. Regional cooperation and exchange of information, as well as a common approach to this problem through joint investigations and establishment of Joint Investigation Teams (JIT), including establishment of an Operational Task Force (OTF), through cooperation with EUROPOL and EUROJUST are crucial for a more effective response to these problems. Development of risk analysis was recognised as a very important tool that could make significant contribution to more efficient identification of threats and their level, further planning, and to more rational use and direction of human resources, which are certainly in short supply. In addition to this approach, it is important to strengthen the investigative capacity of the competent authorities through the acquisition of specialised equipment and training of staff. It was noted that Serbia and Bosnia and Herzegovina are under the greatest pressure from irregular migration, especially considering that these economies share a border/boundary with the external borders of the EU and Schengen on the route of irregular migrants towards the EU.

The use of legal pathways of arrival by migrants in the WB can be viewed from two perspectives that have a significant impact on border/boundary security and migration management. First of all, it should be emphasized that visa policy is an important segment of comprehensive migration management, which plays an important role in preventing and curbing irregular migration. Recently, the economies of the WB have been facing labour shortages due to the emigration of young people to EU member states, and due to strong pressure from employers this shortage is being compensated by bringing in migrant workers from visa-regime economies. Due to urgent needs, clear procedures for verifying the real reasons for the arrival of these migrant workers may not have been established, and it happens that some of them disappear from their jobs soon after their legal arrival in the WB economies and go illegally to the EU member states, creating additional pressure on the border/boundaries. However, there have also been cases where migrant workers, after arriving and starting work, have become victims of human trafficking through labour exploitation. On the other hand, the inconsistency of visa policy of the WB economies with the EU visa policy has also been highlighted in the part of granting visa-free regime to certain economies whose citizens, after legally entering the WB economies, try to illegally reach the EU member states, which results in additional pressure on the border/boundaries. Albania's experience after the revision of its visa policy was very positive, and with such an approach it managed to take steps to prevent irregular migration.

A particular problem is the inability to adequately communicate with migrants due to the lack of interpreters for certain rare languages, and to establish their identity due to the lack of documents. Cooperation with embassies and competent authorities in countries of origin, both in the process of establishing identity and in the process of readmission and return, is not at a satisfactory level. The lack of signed readmission agreements or memoranda of understanding with countries of origin of irregular migrants was highlighted as an additional challenge and obstacle to return. In the context of more efficient cooperation with countries of origin in the identification and readmission procedures, the Readmission Case Management System (RCMS) was also mentioned as a very useful tool used by many EU member states which significantly speeds up these procedures. The importance of involving Ministries of Foreign Affairs in these processes and the contribution they can make was recognised as very important. Although the Assisted Voluntary Return and Reintegration programmes (AVRR) were highlighted as important in the processes of returning migrants to their countries of origin, the detention of migrants and forced removals have proved to be an important means of preventing irregular migration. The particular importance of biometric processing and photographing of migrants was underlined, with the aim of sharing data and establishing identity, and with the support of advanced AI technologies allowing for the detection of persons of security interest. The experiences and best practices of EU member states and FRONTEX in the design and implementation of these procedures would be very important for the WB economies. Regional cooperation on readmission and return, i.e., the implementation of signed readmission agreements in the WB, was assessed as insufficient.

9th Annual Regional Security Coordination Conference in the Western Balkans
Working Together in Times of Global Uncertainties
7-8 November, Sarajevo

*The 9th Regional Security Coordination Conference dubbed "Working Together in Times of Global Uncertainties," on 7 November 2024 in Sarajevo (Photo: RCC/Jasmin Sakovic)*

The WG also addressed the issue of corruption in the context of border/boundary security and migration management, noting that this phenomenon remains significant and can have far-reaching security consequences if more effective ways are not found to prevent corruption and to punish corruption-related crimes more severely.

The need for specialised training and education was considered very important, especially in view of the new trends and changes in the dynamics of the work of criminal groups, where significant support can be provided by FRONTEX and CEPOL, as well as EU and bilateral projects. The problem of police officers leaving the structures due to not so good working conditions was also generally highlighted, as well as the problem of promotion in police structures, where police officers, upon reaching a higher rank, move to other organisational units to perform different tasks, thereby losing their expertise in a specific area.

The lack of political will to address certain security issues more effectively, both at the level of individual economies and at the level of WB, is one of the major challenges. Political will, but also responsibility, is reflected in the fact that strategic documents, action plans, laws and other regulations have not been timely adopted. Certain documents that would strengthen the internal structure of law enforcement agencies and increase the level of operability and readiness to respond to new security risks and threats have also not been adopted due to a lack of political support. The lack of political responsibility is also reflected in the fact that the budget does not provide sufficient funds for strengthening the capacities of competent authorities, increasing salaries and benefits, creating better working conditions and purchasing specialised equipment, as the authorities rely on EU support through various EU or bilateral projects. However, sometimes the needs of competent authorities are not clearly identified for support through various EU projects. On the other hand, it is evident that several different regional and bilateral EU projects are carrying out their activities in the WB where care should be taken to avoid overlapping activities.

It can be said that there is currently no common and coordinated approach among the Western Balkan economies to address these phenomena effectively. Few specialized activities have been recorded in this direction, and there appears to be a limited willingness to identify and tackle the underlying shortcomings and challenges thoroughly. However, the IISG project, as an external initiative for the WB, stands out as a positive example of how some of these efforts can be streamlined and progress can be made through a structured and collaborative framework. Taking into account the EU integration processes of WB economies, EU Delegations in the region can play an important role in coordinating harmonisation of the approaches of all WB economies to these important issues, with the support of EU regional projects. There has been some progress, at least in terms of participation in high-level regional conferences, where decisions are made and specific documents are adopted that commit to resolving specific issues, but their greater implementation is still lacking. In the area of operational cooperation, progress has been made, particularly with regard to conducting joint investigations and concluding agreements on the establishment of Joint Investigation Teams (JITs), as well as Operational Task Force (OTF), which has proved effective in operational actions to identify and arrest criminals, and in which the competent prosecutor's offices have also played an important role.

Cooperation with EU institutions and agencies was considered key in all these processes, with particular emphasis on cooperation with FRONTEX, EUROPOL and EUROJUST. Albania has had very positive experiences after signing the agreement with FRONTEX and deploying its forces to the border/boundary, as with their help it has been able to significantly reduce illegal border/boundary crossings. Albania is also implementing the readmission agreement with Greece to a good extent. In terms of cooperation and exchange of information and coordination of police actions, EUROPOL is a key link, in particular through the EMPACT framework. From the point of view of cooperation and exchange of information, the work with liaison officers and police attachés was recognised as very important. EU support in the area of strengthening the capacity of competent authorities through the procurement of specialised equipment, organisation of specialised training, expertise and exchange of best practices, including strengthening regional cooperation, remains crucial, especially in view of the pronounced budgetary constraints in the WB economies.

## 2.1.3 Overall Recommendations

The need for stronger political will and support for relevant institutions in all aspects of their work in WB economies was emphasized. It would also be good to focus on developing a sense of shared responsibility and commitment in the WB, while strengthening mutual trust.

**Common WB Approach:** Harmonise visa policy of WB economies with the EU visa policy; take steps towards a common, coordinated approach by WB economies to border/boundary security and migration management issues through harmonisation of strategies, action plans and legislation; and explore the possibilities of developing a common SOCTA, strategy and plans.

**Border/Boundary Security:** Strengthen the overall concept of Integrated Border Management, develop and further strengthen risk analysis; blockage of places suitable for illegal border/boundary crossing and transportation of illegal goods; strengthen cross-border/boundary cooperation through joint patrols and meetings; building, equipping and establishing joint border/boundary crossings; improving the work and exchange of information through Police Cooperation Centres; establish and strengthen cooperation with FRONTEX through deployment of its forces at the border/boundary, exchange of best experiences and practices.

**Capacity Building:** Acquiring specialised equipment and new technologies for more efficient border/boundary crossing control and surveillance; acquisition of advanced biometric identification and facial recognition systems for a more efficient way of registration and identification of migrants in an irregular situation; acquisition of specialised equipment to strengthen criminal investigation capabilities; organisation of joint WB training courses on the use of specialised equipment for border/boundary surveillance, detection of forged documents, passenger profiling, investigative techniques, biometric systems and human rights with a focus on training of trainers in cooperation with Frontex and CEPOL and with the support of EU and bilateral projects.

**Readmission and Return:** Improve the implementation of readmission agreements between the Western Balkan economies; improve cooperation with countries of origin by signing readmission agreements or memoranda of cooperation; improve cooperation with countries of origin of irregular migrants on identity verification procedures, in particular by examining the possibility of introducing and using the Readmission Case Management System (RCM), consider the possibility of organising joint return flights to remove migrants residing in WB economies in an irregular status.

**Cooperation with International and Non-governmental organisations:** Strengthen cooperation with international and non-governmental organisations in providing various services to migrants in centres, working with vulnerable categories of migrants, identifying victims of human trafficking, placing them in safe houses and their further protection, as well as cooperation in AVRR procedures.

**Labour Migration:** Adopt a more effective policy on the arrival of migrant workers in the Western Balkan economies, with a coordinated approach and cooperation between competent authorities in the selection of migrant workers, with the aim of: more effective profiling of workers in the country of origin who will not attempt to emigrate illegally to EU member states after legal arrival; better information of migrant workers on their rights and obligations in order to prevent the possibility of becoming victims of human trafficking through labour exploitation.

**Regional and EU Cooperation:** Improve cooperation amongst the competent authorities of the Western Balkans through regular meetings, conferences, workshops, exchange of best practices and experiences; strengthen the investigative capacity of Western Balkan competent authorities, and cooperation and coordination with EUROPOL through information exchange, conducting joint investigations, establishing Joint Investigation Teams (JITs) and working in the Operational Task Force (OTF); increase the involvement and participation of competent authorities of the Western Balkans in EMPACT activities.

# 2.2 WORKING GROUP 2 REPORT: COUNTERING ORGANISED CRIME AND CORRUPTION IN THE WESTERN BALKANS

**Author: Prof. Trpe Stojanovski,**

**Senior Advisor GI-TOC**

> *"The top five issues that impact security in the Western Balkans are economic situation, corruption, depopulation, organised crime, and governmental leadership. Citizens believe the Western Balkans is not a secure region, and the threat of a potential war is present… (Majlinda Bregu:2024)"*

**Keywords**

Security threats, security issues, local challenges, digital crime, organised crime, criminal networks, transnational organised crime, crime prevention, corruption, anti-corruption measures, international treaties, law enforcement, law enforcement integrity, political will, trust building, regional cooperation, international cooperation, operational cooperation, inter-agency cooperation, police collaboration, information exchange, capacity building, training, monitoring, leadership.

## 2.2.1 Introduction

Organised crime and corruption are two most significant challenges threatening the Western Balkans' stability, security, and development. The region's geographic location, at the crossroads of Europe, makes it a key transit route for transnational criminal activities such as drug and arms trafficking, human trafficking and smuggling, and money laundering. These activities are further exacerbated by systemic governance challenges, institutional weaknesses, and political interference, creating fertile ground for criminal networks to operate with impunity.

*Prefetto Stefano Gambacurta, Deputy Director General of Public Security, Ministry of Interior, Italy, at the 9th Regional Security Coordination Conference dubbed "Working Together in Times of Global Uncertainties," on 7 November 2024 in Sarajevo (Photo: RCC/Jasmin Sakovic)*

These issues deeply affect the socio-economic fabric of the Western Balkans. Weak public institutions, widespread corruption, and an informal economy enable organised crime and diminish public trust in the rule of law and the government's ability to address these threats effectively. Furthermore, the region's unresolved political tensions and historical conflicts contribute to an environment where insecurity persists, and cooperation between economies is inconsistent.

Corruption remains pervasive, undermining judicial and law enforcement institutions and limiting their capacity to combat organised crime. Low conviction rates for high-profile corruption and criminal cases have eroded public trust and fuelled a sense of impunity among criminal networks. Meanwhile, economic vulnerabilities such as unemployment and a lack of opportunities drive migration and depopulation, further weakening the region's resilience.

In this complex landscape, on 8th November 2024 in Sarajevo the Working Group 2 Countering Organised Crime and Corruption in the Western Balkans brought together 23 experts and decision-makers from 6 law enforcement agencies of the WB participants, regional organisations, and international bodies such as EUROPOL, INTERPOL, SELEC, RAI, GI TOC and the European Commission, as well as police officers from Italy and Turkey. This collaborative platform addressed organised crime's root causes and enablers, enhanced regional and international cooperation, and developed strategies to strengthen governance, integrity, and institutional accountability.

The Working Group 2 emphasised the importance of gender and diversity inclusion, recognising the untapped potential of women and underrepresented groups in strengthening the effectiveness of law enforcement agencies.

As the Western Balkans faces increasing global uncertainties, fostering regional cooperation, addressing systemic corruption, and building institutional resilience, remain critical to ensuring security and sustainable development for the region and its neighbours. This report consolidates the Working Group 2 key insights, challenges, and recommendations, providing a roadmap for collaboratively addressing organised crime and corruption.

## 2.2.2 Drivers of Organised Crime

**Institutional Weaknesses and Economic Vulnerabilities**: The Western Balkans faces significant governance challenges, including limited resources, political interference, and a lack of robust regulatory frameworks. These institutional weaknesses create fertile ground for organised crime to flourish. Economic vulnerabilities, such as high unemployment rates, informal economy, and sectors prone to illicit activities like construction and casinos, further exacerbate the problem. Organised crime groups exploit these vulnerabilities to launder money, evade taxes, and engage in other criminal activities.

**Cross-Border/Boundary Complexities**: The Western Balkans' geographic location at the crossroads of Europe and Asia makes it a key transit route for transnational criminal activities. Criminal networks leverage regional borders/boundaries to facilitate cross-border/boundary illicit activities, taking advantage of inconsistencies in laws and enforcement mechanisms. This cross-border/boundary nature of crime necessitates a coordinated regional response.

**Examples from the Working Group 2**: Participants highlighted how high-profile sectors like casinos are used for laundering significant sums of money. Organised crime syndicates utilise fake companies to evade taxes and launder money across border/boundaries, making detection and prosecution difficult. The Working Group 2 also discussed the role of corruption in enabling organised crime, with law enforcement often directly involved in criminal activity or control of local markets.

**Recommendations**:

- **Strengthen Governance Frameworks**: Introduce regulatory reforms to address vulnerabilities in high-risk economic sectors. Implement financial monitoring systems to detect illicit flows early.
- **Enhance Cross-Border/Boundary Collaboration**: Establish regional task forces focusing on intelligence sharing and joint operations. Increase collaboration through platforms like Europol's SIENA and Interpol databases.
- **Focus on Economic Crime Training**: Provide specialised training for law enforcement to identify and investigate complex economic crimes.

## 2.2.3 Corruption and Oversight

**Systemic Corruption**: Political interference in law enforcement and judicial processes leads to dropped investigations and low conviction rates, eroding public confidence. The lack of harmonised oversight frameworks creates accountability gaps, allowing corruption to thrive. Corruption and organised crime are mutually reinforcing, leading to systemic weaknesses in the rule of law.

**Examples from the Working Group 2**: The vetting process was cited as a successful initiative to improve police integrity. However, limited progress in confiscating criminally acquired assets was noted as a critical shortfall. The Working Group 2 emphasised the need for targeted risk assessments and dedicated measures to address corruption in vulnerable sectors.

**Recommendations:**

- **Establish Harmonised Oversight Mechanisms**: Create independent anti-corruption bodies to monitor law enforcement and judicial activities. Use the experience of countries with successful vetting models.
- **Confiscation of Assets**: Develop streamlined procedures for confiscating and redistributing criminally acquired assets, ensuring transparency.
- **Capacity Building**: Conduct workshops and training programmes on detecting, preventing, and investigating corruption within law enforcement.

## 2.2.4 Regional and International Cooperation

**Challenges in Regional Cooperation**: Political interference, institutional silos, and varying legal standards hinder effective collaboration. The inability to access economy-level databases was highlighted as a significant barrier. The Working Group 2 underscored the importance of regional cooperation for stability and economic development.

**Strengthening Inter-Agency Cooperation**: Successful examples, such as using cadastral data in investigations, demonstrate the potential of shared resources. However, platforms like Europol's SIENA and Interpol's I-24/7 are underutilised, indicating a need for greater regional ownership and coordination.

**Recommendations**:

- **Expand Task Forces**: Establish specialised cross-border/boundary task forces to address region-specific crimes.
- **Secure Digital Platforms**: Create secure regional digital platforms for real-time intelligence sharing.
- **Capacity-Building Programmes**: Organise joint training workshops for regional law enforcement officers and public prosecutors.

## 2.2.5 Technological and Digital Competence

**Digital Forensics and Big Data Analysis**: A critical capacity gap was identified within law enforcement agencies. Criminal networks' growing use of encrypted communications necessitates a robust technological response. The Working Group 2 emphasised the need for digital transformation to enhance law enforcement capabilities.

**Recommendations**:

- **Invest in Training**: Organise digital forensics and data analysis workshops, focusing on emerging threats like cryptocurrency fraud.
- **Leverage Existing Platforms**: Promote the use of Europol's SIENA and Interpol's I-24/7 systems for intelligence sharing.
- **Create Regional Digital Crime Centres**: Establish digital forensics labs with state-of-the-art technologies.

## 2.2.6 Gender and Diversity Inclusion

**Empowering Women and Promoting Diversity**: Gender inclusion and women empowerment in law enforcement are critical for enhancing institutional effectiveness. The Working Group 2 highlighted the need for greater representation of women in leadership positions and the inclusion of underrepresented groups.

**Challenges in Gender Representation**: Cultural and institutional barriers limit the inclusion of women in leadership positions. The Working Group 2 addressed these barriers to foster a more inclusive and effective law enforcement environment.

**Recommendations**:

- **Mentorship and Training Programmes**: Create mentorship programmes to prepare women for leadership roles.
- **Diversity Metrics and Benchmarks**: Integrate gender-focused metrics into recruitment and performance evaluations.
- **Cultural Change Initiatives**: Conduct awareness campaigns within law enforcement institutions to highlight the value of diversity.

## 2.2.7 Conclusion

The 9th Annual Regional Security Conference in the Western Balkans successfully brought together diverse stakeholders to address the multifaceted challenges of organised crime and corruption.

The Working Group 2 illuminated systemic vulnerabilities perpetuating criminal networks and undermining regional governance through dynamic discussions and collaborative exchanges. The Western Balkans' geographic location and socio-economic challenges necessitate a concerted effort to bolster institutional integrity, enhance technological capacity, and foster regional and international cooperation.

The Working Group 2 provided a collaborative platform for key stakeholders, including regional law enforcement, international organisations, academia and civil society, to share insights and develop actionable strategies. The Working Group 2 underscored that tackling organised crime requires strong governance frameworks, legal reforms, and significant investments in capacity building and technological advancements. From adopting advanced digital forensics tools to addressing cross-border/boundary operational gaps, the findings highlight the importance of a modernised approach to law enforcement. Moreover, participants emphasised the value of regional collaboration through initiatives such as joint task forces and intelligence-sharing platforms, which are indispensable in countering transnational organised crime.

An equally significant theme was the inclusion of gender and diversity in security agencies. Promoting equal representation and leadership opportunities for underrepresented groups is a matter of equity and a strategic advantage for enhancing institutional effectiveness. The Working Group 2 focus on fostering cultural change within law enforcement agencies is essential to building trust and legitimacy.

MINISTERO
DELL'INTERNO
RegionalCooperationCouncil
Ministry of Foreign Affairs and International Cooperation
9th Annual Regional Security Coordination Conference in the Western Balkans
Working Together in Times of Global Uncertainties
7-8 Nove r, Sarajevo

*H.E. Mr. Luigi Soreca, Ambassador, Head of the Delegation of the European Union to Bosnia and Herzegovina, at the 9th Regional Security Coordination Conference dubbed "Working Together in Times of Global Uncertainties," on 7 November 2024 in Sarajevo (Photo: RCC/Jasmin Sakovic)*

As the region faces increasing global uncertainties, sustained political commitment, public trust, and regional solidarity will be the cornerstone of progress. By implementing the recommendations outlined, the Western Balkans can create a more secure and resilient environment for its citizens. This Working Group 2 marks not an endpoint but a pivotal step towards a future where integrity, accountability, and cooperation define the region's approach to combating organised crime and corruption. RCC has a unique cohesive role to drive the process in the future.

## 2.2.8 Recommendations

The 9th Annual Regional Security Conference recommendations for the Western Balkans emphasise a comprehensive approach to combating organised crime and corruption in the region. To enhance information sharing, it is crucial to increase local law enforcement's access to Europol's SIENA platform and expand training programmes focused on intelligence sharing. Strengthening regional cooperation involves establishing regional centres for joint investigations and data analysis, developing standardised protocols for cross-border/boundary operations, and creating a regional Serious and Organised Crime Threat Assessment (SOCTA) document tailored to the Western Balkans.

Building technological capacity is another critical area, requiring investments in advanced digital forensics and encrypted communication analysis tools. Additionally, frontline officers must receive enhanced training in technology used to address emerging threats effectively. Promoting diversity within law enforcement is equally important, with recommendations to implement recruitment campaigns to increase women's participation and support leadership development programmes for underrepresented groups.

Looking ahead, future directions include aligning regional policies with EU directives and best practices to create a unified strategy. Establishing training centres for digital forensics and financial investigations is essential, alongside investments in digital knowledge and dedicated centres for detecting and documenting digital crime. Finally, mechanisms for monitoring and evaluating reforms are necessary to ensure continuous improvement and effective implementation of these strategies. The Western Balkans can strengthen institutional integrity, foster cooperation, and build resilience against organised crime and corruption by addressing these areas.

Based on the future directions and discussions outlined in the Working Group 2, additional recommendations can be formulated to address the challenges of combating organised crime and corruption in the Western Balkans. Firstly, there is a need to prioritise the alignment of regional policies with EU directives and best practices to establish a unified strategy that ensures consistency and fosters cooperation across borders/boundaries. This alignment would streamline efforts and enhance the effectiveness of regional initiatives. Secondly, investments should be made in capacity building by establishing specialised training centres for digital forensics and financial investigations. These centres would equip law enforcement agencies with the necessary skills to combat emerging threats and provide a platform for continuous learning and adaptation to technological advancements.

Moreover, enhancing digital knowledge within law enforcement institutions should be a priority, alongside creating dedicated centres for detecting and documenting digital crimes. These measures would address the growing sophistication of criminal networks that exploit digital platforms. Lastly, mechanisms for monitoring and evaluating reforms must be developed to ensure accountability, track progress, and enable timely strategy adjustments. Such mechanisms would foster transparency and support continuous improvement in effectively addressing organised crime and corruption. By implementing these additional recommendations, the Western Balkans can strengthen their institutional resilience and create a more secure and stable environment.

# 2.3 WORKING GROUP 3 REPORT: COUNTERING CYBER THREATS IN THE WESTERN BALKANS

**Author: Metodi Hadji-Janev, PhD,**

**Associate Law Professor at the General Mihailo Apostolski Military Academy in Skopje**

## 2.3.1 Introduction

Comprising 18 members from the Western Balkans, and additional participants from Moldova, Italy, and EUROPOL, Working Group (WG) 3 addressed security challenges and considerations streaming from cyberspace. The working framework initial assumption for WG 3 was the notion that the advancement of digitalisation accelerates the convergence between cyber and physical space. At the same time, the WG 3 worked under the consideration that cybersecurity emerges as an important factor for both human and economy-level security. Although digitalisation and emerging technologies have many positive aspects - introducing benefits that may improve well-being across various societal sectors, if not matched by a parallel focus on security these processes may also introduce many threat vectors. Therefore, in an era of digitalisation, emerging technologies, and hybrid threats, cybersecurity is crucial for the Western Balkans. It safeguards against cybercrime, protects sensitive data and defends against cyber espionage targeting critical information infrastructure. Moreover, with increased geopolitical tensions and the rise of organised crime exploiting digital vulnerabilities, robust cybersecurity measures are vital to ensuring regional stability and resilience in the face of evolving threats.

This framework reflected the primary goal of the RCC's 9th Regional (Jumbo) Security Coordination Conference, i.e., "strengthening of the regional cooperation and resilience by fostering a collaborative approach to security challenges". Hence, the WG 3 facilitated the conference in achieving greater awareness of the necessity to align regional cyber security mechanisms with the EU standards in order to ensure a stable and secure future for the Western Balkans. Additionally, the WG 3 provided a platform for regional stakeholders to update each other on the current work, needs and future engagement. For this purpose, the RCC Secretariat provided structured questions to guide discussions, yielding targeted insights and outcomes.

Questions were aligned with the overall objectives of the upcoming 9th Regional Security Coordination Conference and echo the ambition to instigate debate that will support the spirit of Working Together in Times of Global Uncertainties. They were separated into two sets of which  the first set focused on the growing threats of cyber-attacks, hybrid warfare, the impact of emerging disruptive technologies (such as AI, quantum computing, and autonomous systems) on regional security and the need for robust regional and European cooperation to counter these threats. The second set focused on the necessity to align WB cybersecurity frameworks with European best practices through cybersecurity governance, risk and compliance. Both sets of questions instigated in-depth discussion and helped extract valuable insights for forming tailored policy recommendations.

## 2.3.2 Overview of the morning session discussion – addressing the first set of questions

The WG 3 identified numerous pressing issues in cybersecurity relevant to all WB economies. These issues could best be systemised as follows: limited cybersecurity resources and capacity; underdeveloped regulatory frameworks and enforcement mechanisms; and increasing sophistication of cyber threats. These factors underscore the need for enhanced cybersecurity investments, cooperation, and training to effectively address the specific challenges faced by the Western Balkans.

One of the main conclusions was that the region is facing limited cybersecurity resources and capacity. Participants were united in the sense that most Western Balkan economies face resource constraints, including insufficient funding, limited skilled personnel, and outdated infrastructure. This makes it difficult to build robust defences against cyber threats and respond effectively to incidents.

Underdeveloped regulatory frameworks and enforcement mechanisms were also discussed as a serious challenge. While many economies are aligning with EU cybersecurity standards, some lack fully established legal and regulatory frameworks. Even where these frameworks exist, enforcement can be inconsistent due to limited governmental cybersecurity expertise and politicisation of cybersecurity sector.

The Working Group 3 concluded that the sophistication of cyber threats is constantly growing. Threat entities are constantly evolving their tactics, often outpacing regional defences. The rise of ransomware attacks, data breaches, and phishing campaigns highlights the need for stronger preventive measures and incident response capabilities. Hence, public-private partnership (PPP) and regional cooperation are of paramount importance because in cyberspace no one is safe alone.

Participants also shared some experiences from past incidents to support their thesis.

Cyber-attack on Montenegro (2022) was one of the significant attacks that was mentioned either as a reference or certain aspects were used as an example several times during the discussion in both sessions. Montenegro experienced a significant cyberattack that targeted multiple government systems, disrupting

MINISTERO DELL'INTERNO
RegionalCooperationCouncil
9th Annual Regional Security Coordination Conference in the Western Balkans
Working Together in Times of Global Uncertainties
Sarajevo

*Cons. Thomas Botzios, Director for the Adriatic and Balkans, the General Directorate for the European Union, Ministry of Foreign Affairs and International Cooperation, Italy, at the 9th Regional Security Coordination Conference dubbed "Working Together in Times of Global Uncertainties," on 7 November 2024 in Sarajevo (Photo: RCC/Jasmin Sakovic)*

services and leading to substantial costs in recovery efforts. This incident revealed vulnerabilities in economy's cybersecurity infrastructure and had implications on its security, as it involved potential espionage from a hostile entity. The attack had a multi-layered footprint.

Cyber incidents in the financial sector, particularly against banks, have caused disruptions, financial losses, and reduced public trust in digital banking services. Such breaches affect economic stability, as they can weaken consumer confidence and harm the reputation of regional institutions. Critical infrastructure, such as energy and telecommunications, has been a target, with attacks disrupting services and exposing vulnerabilities that could impact economy-level security if exploited further.

Participants also suggested that unique regional vulnerabilities were exploited by cybercriminals or hostile state entities on several other occasions across the region affecting institutions that were highly vulnerable and rich with citizens' data. These attacks showed high levels of digital vulnerability in the public and private sectors. Many organisations across sectors have low levels of cyber hygiene, creating easy access points for cybercriminals. The use of outdated systems, unpatched software, and lack of multifactor authentication in both public and private sectors increases susceptibility to attacks.

Cooperation in cybersecurity is highly fragmented. While there are efforts to enhance cross-border/boundary collaboration, limited data-sharing agreements and a lack of coordinated incident response frameworks make it easier for cybercriminals to exploit vulnerabilities across border/boundary.

Political and ethnic tensions generate unique challenges for the region. The region's ethnic and political complexities make it susceptible to cyber-enabled information warfare and disinformation campaigns. Hostile entities, including some state-sponsored groups, often use cyber means to exploit these divisions, further destabilising public trust.

As the WB's cyber security trends are not in a vacuum, the WG 3 also addressed the geopolitical factors affecting cyber threat levels in the Western Balkans. Along these lines, several key points were identified as important by the WG 3 members.

Proximity to conflicting geopolitical interests reflects the evolving nature of cybersecurity threats to the region. The Western Balkans is at the crossroads of influence from major powers, including the EU, Russia, and China. These dynamics often result in cyber campaigns aimed at swaying political allegiances or undermining regional stability. Cyber threats are, therefore, both an economy-level and geopolitical issue.

NATO and EU aspirations of the region's economies mostly drive foreign influence. Some economies in the region are in the process of joining NATO and most of the economies attempt to align with the EU. This shift attracts cyber threats from states that see these moves as adversarial. Consequently, state-sponsored entities often conduct cyber espionage to disrupt this alignment.

Hence, exploiting cyberspace and modern transformative technologies for disinformation and destabilisation is increasing across the region. Hostile entities may leverage the Western Balkans' online spaces for disinformation campaigns to exacerbate social divisions and erode trust in institutions. These campaigns are increasing the cybersecurity challenge, impacting public perception and posing risks to democratic processes.

In the context of regional cooperation, the WG 3 observed that Western Balkan economies can improve coordination by establishing unified standards for cybersecurity and creating joint incident response teams. Integrating with EU cyber initiatives, such as the European Union Agency for Cybersecurity (ENISA), can also enhance information sharing, capacity-building, and coordinated responses to cross-border/boundary cyber threats. However, regional initiatives and organisations such as RCC can help in establishing a real regional footprint in cyber security efforts and reflect unique cross-cultural issues for the WB economies.

Existing frameworks such as the Western Balkans Digital Agenda and Regional Cooperation Council (RCC) could be strengthened by increasing funding for regional cybersecurity projects, expanding training programmes, and fostering deeper data-sharing protocols across borders/boundaries to improve threat intelligence.

On the question of the main barriers to effective regional cybersecurity cooperation participants believe that the key barriers include limited funding, varying cybersecurity capacities amongst the economies, political differences, and a lack of harmonised regulatory frameworks. Additionally, trust issues and the absence of formalised data-sharing agreements hinder comprehensive regional coordination.

One successful model that could be a leading example to boost cooperation across the region is the Cybersecurity Public-Private Partnership (PPP) initiative in Serbia, which fosters collaboration amongst government, industry, and academia on cybersecurity training, awareness, and innovation. Other initiatives, like Albania's public-private sector partnership, are dedicated to strengthening the economy's cybersecurity culture and fostering trust through collaboration. This and similar approaches support development of a clear cybersecurity action plan and enhance infrastructure efficiency by improving cybersecurity protections across the economy.

Addressing hybrid threats via cyberspace, participants agreed that hybrid threats in the Western Balkans are increasingly sophisticated, combining cyberattacks with disinformation campaigns targeting ethnic and political divisions. These campaigns often seek to exploit social vulnerabilities to fuel distrust in institutions and destabilise governments. Cyber-enabled disinformation targeting elections and public health crises are prominent examples of this evolving threat.

Some of the Foreign state entities are known to engage in cyber espionage, disinformation, and influence campaigns in the Western Balkans to sway political allegiance or undermine EU/NATO integration. To build resilience, the region needs to enhance threat intelligence sharing, improve cybersecurity education, and establish clearer coordination frameworks with international allies.

For these purposes, the governments need to take significant stapes to counter cyber-enabled election interference and political manipulation. Governments need to invest in election cybersecurity and implementing secure digital voting systems and training of election officials on cyber hygiene. Additionally, counter-disinformation measures, such as monitoring social media for false narratives, public awareness campaigns, and stronger partnerships with tech platforms, are crucial to mitigate manipulation and maintain electoral integrity.

Tackling the ways in which emerging technologies may pose security risks in the Western Balkans, participants concluded that emerging technologies like AI, quantum computing, and autonomous systems introduce various and increasing risks. This includes but is not limited to AI-driven cyberattacks, increased data breaches, and threats to encryption standards from quantum computing. AI could be exploited to automate large-scale disinformation campaigns, while quantum computing may eventually compromise existing encryption, making sensitive data vulnerable across critical sectors.

However, participants also opted that these technologies may be an opportunity for regional economies. Therefore, some suggested that harnessing emerging technologies could help in establishing better cybersecurity defences. Western Balkan economies can use AI for advanced threat detection, predictive analytics, and automated responses to cyber threats. Quantum-resistant encryption could be adopted proactively to protect against future quantum risks. Implementing these technologies alongside robust policies can help mitigate potential misuse.

International partners and private sector can provide critical expertise, funding, and technology transfers. Collaboration on pilot projects, knowledge exchange, and training initiatives can strengthen the region's adaptation to these emerging threats. Private sector partnerships, particularly with tech companies, are also essential for developing and implementing advanced cybersecurity solutions tailored to the Western Balkans' specific needs.

# 2.3.3 Overview of the discussion, conclusions and recommendations of the second session

The second session built on the outcomes from the first session and addressed the governance, risk and compliance aspects of cybersecurity.

This session aimed to explore how regional frameworks align with the EU and the global best practices, manage risk, and ensure compliance with international and European standards. During the session participants also tried to explore how crosscutting themes such as good governance and GESI aspects are addressed in the Western Balkans policies through the governance, risk, and compliance mechanisms.

Cybersecurity governance in the Western Balkans is largely underdeveloped, with varying levels of integration across economy-level frameworks. Some economies have established cybersecurity agencies or designated authorities to oversee cybersecurity strategies, but coordination across ministries and with the private sector often remains fragmented. This fragmentation can limit the effectiveness of cybersecurity policies and incident response capabilities, emphasizing the need for clearer economy-level governance structures and interagency cooperation.

Several Western Balkan economies are beginning to incorporate good governance principles, including transparency and accountability, into their cybersecurity frameworks. However, gender equality and social inclusion (GESI) considerations are less consistently prioritised. Some initiatives, often funded by international organisations, include training and capacity-building programmes that promote GESI by encouraging women's participation in cybersecurity roles and fostering inclusivity in policy-making. More institutionalised mechanisms, such as dedicated GESI benchmarks in economy-level strategies, would help ensure sustained progress.

Economies in the Western Balkans are making strides in aligning with EU cybersecurity standards as part of their EU integration efforts. For example, many have introduced cybersecurity strategies and adopted frameworks inspired by the EU's Network and Information Security (NIS) Directive and the EU Cybersecurity Act. However, full compliance remains a work in progress, as economies face challenges in terms of regulatory resources, enforcement capabilities, and alignment across sectors.

Participants recognised the role of regional organisations, such as the Regional Cooperation Council (RCC), in bridging some of the identified gaps**.** Regional organisations like the RCC are essential for supporting cybersecurity policy alignment and capacity-building between the Western Balkans and the EU. The RCC can provide platforms for dialogue, foster regional collaboration, and support the adoption of EU-aligned cybersecurity standards. Additionally, the RCC can facilitate knowledge sharing and joint projects, which help address operational gaps by pooling resources, coordinating cybersecurity training, and standardising policies across the region. Along these lines, it was suggested that a regional cyber security fellowship as a regional footprint in cybersecurity could be a viable option and an example to foster regional cooperation in this context.

Western Balkans' risk assessment frameworks are at varying levels of maturity. Some economies have adopted structured frameworks to assess and manage cybersecurity risks, often aligned with EU standards or international guidelines. However, updates to these frameworks may be irregular due to limited resources and evolving threats, highlighting the need for more systematic and frequent revisions to adapt to the rapid pace of cybersecurity risks.

While most Western Balkan economies have defined roles for incident response, coordination - both at economy and at regional level - can be inconsistent. Economy-level cybersecurity agencies or designated CSIRTs (Computer Security Incident Response Teams) typically handle incident responses, but interagency collaboration and cross-border/boundary coordination are often limited. Enhanced regional partnerships and regular joint exercises would improve the effectiveness and speed of responses.

Given that cybersecurity plays a role in economic, political and social dynamics of governance, the influence of economic, political, and social factors on cybersecurity risk management was also considered. Economic constraints limit investments in cybersecurity infrastructure, particularly in smaller economies within the region, which impacts risk management capabilities. Political priorities can also shift attention away from cybersecurity, while social factors, such as low cybersecurity awareness, may increase vulnerabilities. Effective risk management requires stable investments, political commitment, and public awareness to build a culture of cybersecurity resilience.

Aligning to the conference objective, the Working Group 3 could have not avoided the impact that good governance, corruption, and organised crime may have on cyber resilience**.** Good governance is crucial for strong cybersecurity, as it supports transparency, accountability, and effective policy implementation. Corruption and organised crime, however, can undermine these efforts by weakening institutions, reducing trust, and creating vulnerabilities that cybercriminals or hostile entities may exploit. Addressing these issues and building institutional integrity are essential for strengthening risk management frameworks and enhancing cyber resilience in the region.

Participants were united in the importance of the adoption of internationally recognised cybersecurity frameworks like ISO 27001 and NIST across the Western Balkans. While larger organisations and institutions, especially in finance and telecommunications, are more likely to implement these frameworks, adoption is less common amongst small and medium-sized enterprises (SMEs) due to resource constraints and limited awareness. Increasing adoption rates could be achieved through government incentives, public awareness campaigns, and training programmes that emphasize the benefits of standardised cybersecurity practices.

To promote cybersecurity certifications for both organisations and individuals, the region could benefit from subsidising training programmes, creating clear pathways for professional certification, and collaborating with educational institutions. Establishing partnerships with international organisations could also help provide affordable access to certification courses, making it easier for individuals and organisations to pursue recognised qualifications.  A regional certification initiative, especially if aligned with EU standards, would be highly valuable for enhancing compliance and standardisation across the Western Balkans. Such an initiative could involve creating a shared regional certification body or incentivising compliance through tax breaks, grants, or reduced regulatory requirements for certified organisations. These incentives could drive a higher standard of cybersecurity, facilitate cross-border/boundary business, and enhance regional cyber resilience by ensuring a consistent level of security across critical sectors.

MINISTERO DELL'INTERNO
DIPARTIMENTO DELLA PUBBLICA SICUREZZA
9th Annual Regional Security Coordination Conference in the Western Balkans
Working Together in Times of Global

*Ms. Federica Mogherini, Rector of the College of Europe and Director of the European Union Diplomatic Academy, implemented by the College of Europe; Former High Representative of the Union for Foreign Affairs and Security Policy, at the 9th Regional Security Coordination Conference dubbed "Working Together in Times of Global Uncertainties," on 7 November 2024 in Sarajevo (Photo: RCC/Jasmin Sakovic)*

## 2.3.4 Policy recommendations

The recommendations were crafted to reflect the insights and diverse perspectives shared during the WB 3 discussions, where participants identified key challenges and opportunities in strengthening cybersecurity across the Western Balkans. They represent an expert vision aimed at fostering regional resilience, grounded in practical steps for governance, risk management, and compliance while enhancing regional and international cooperation. Each recommendation aims to address critical gaps identified by the WG 3, such as the need for stronger cross-border/boundary collaboration, alignment with EU standards, and public-private partnerships that can support comprehensive and effective cybersecurity strategies.

These recommendations, therefore, serve as points to inspire immediate and long-term actions. They are tailored to build on the existing frameworks while fostering innovation, inclusivity, and alignment with international practices. By addressing both current vulnerabilities and emerging threats, the recommendations provide a pathway to elevate the region's cybersecurity posture, ensuring that policy and operational measures are both responsive and forward-looking. They are intended to mobilise stakeholders - governments, private sector, civil society, and international partners - towards shared goals of security, transparency, and digital resilience in the Western Balkans. For a general and more systemised approach recommendations cover thematic areas discussed during the WG 3 sessions.

## 1. Cybersecurity challenges and hybrid threats

- **Develop regional cyber threat intelligence sharing.** Establish a Western Balkans Cyber Threat Intelligence Network to improve real-time threat sharing and incident response. This network should include public and private sectors and connect to the EU's intelligence systems, enhancing visibility of hybrid threats.

- **Strengthen cyber resilience against hybrid threats.** Implement resilience strategies that combine cyber defences with disinformation countermeasures, such as media literacy programmes and fact-checking platforms. Support cross-border/boundary training to enhance each economy's capacity to respond to complex hybrid threats.

- **Increase investment in cybersecurity infrastructure.** Provide financial assistance or incentives for building robust cybersecurity infrastructure, particularly in sectors vulnerable to political manipulation, such as media and electoral systems.

## 2. Regional and European cooperation

- **Establish a Western Balkans cybersecurity coordination body.** Create a formal body to coordinate cybersecurity initiatives, set region-wide standards, and harmonise policies with EU directives like the NIS Directive and Cybersecurity Act..

- **Strengthen legal and policy frameworks for data sharing.** Promote alignment of economy-level laws on data protection and incident reporting, facilitating smoother cross-border/boundary collaboration. A regional protocol for data sharing can also ensure swift responses to emerging threats.

- **Encourage public-private partnerships (PPPs).** Develop a regional PPP framework to promote cybersecurity innovation and resource-sharing between governments, academia, and industry. Case studies from EU member states could be shared to illustrate the benefits of PPPs in cybersecurity.

## 3. Governance in cybersecurity

- **Integrate cybersecurity into economy-level governance structures.** Define cybersecurity roles across government ministries, ensuring a clear chain of command and responsibility for incident response and governance. These roles should be aligned with broader economy-level security policies to create a unified governance structure.

- **Institutionalise good governance and GESI in cybersecurity strategies.** Implement gender equality and social inclusion (GESI) guidelines as part of economy-level cybersecurity policies. Incentivise organisations to incorporate GESI in hiring and governance practices by tying GESI compliance to cybersecurity grants or funding.

- **Align economy-level cybersecurity strategies with EU standards.** Provide resources and technical assistance to harmonise economy-level frameworks with EU standards. Regional institutions like the RCC can facilitate workshops to support the implementation of EU-aligned policies.

4. **Risk management and cyber resilience**

- **Create a unified risk assessment framework:** Establish a regional risk assessment framework based on best practices from ISO 31000 and NIST standards. This framework should be adaptable to each economy's needs and updated regularly to account for evolving cyber threats.

- **Enhance cross-border/boundary coordination for incident response.** Develop a cross-border/boundary incident response protocol with defined roles and responsibilities. Regional incident response exercises could improve coordination and reveal gaps in current processes.

- **Address corruption and organised crime in cyber policies.** Institute stronger checks and oversight mechanisms to prevent cyber-related corruption and address organised crime's influence. This could include transparency protocols for cybersecurity funding, which would foster accountability and deter criminal involvement in cyber operations.

5. **Cybersecurity frameworks and certification**

- **Promote the adoption of international cybersecurity standards.** Offer financial incentives, such as tax breaks or grants, for companies adopting frameworks like ISO 27001 and NIST. Additionally, provide SMEs with free or subsidised training to meet these standards, helping overcome cost barriers.

- **Create a regional cybersecurity certification body.** Establish a Western Balkans certification authority that aligns with EU standards and provides accessible certification programmes. This authority could offer regional certifications and serve as a bridge for Western Balkan economies to meet EU cybersecurity requirements.

- **Support cybersecurity workforce development through certification.** Partner with educational institutions to integrate cybersecurity certification programmes into curricula. Scholarships or subsidies for professional certifications would encourage individual uptake and build the region's cybersecurity talent pool.

6. **Emerging technologies (AI, Quantum Computing, Autonomous Systems)**

- **Develop policies for responsible use of AI and emerging technologies.** Establish guidelines for safe and responsible AI use, prioritising transparency and accountability. Support R&D in quantum-resistant encryption and AI-driven threat detection to harness the benefits of emerging technologies.

- **Collaborate with international partners on emerging tech security.** Engage with EU initiatives and international partners to adopt standards and best practices for emerging technologies. Partnerships with global technology firms and universities can facilitate technology transfer and help the Western Balkans stay current on security trends.

- **Launch an innovation fund for cybersecurity R&D.** Create a regional innovation fund to support local research and development in cybersecurity, focusing on emerging technologies. This fund could offer grants to universities and tech firms developing advanced cybersecurity solutions and position the Western Balkans as a competitive force in the tech sector.

## 2.3.5 Overall Recommendations

- **Create a cybersecurity roadmap for the Western Balkans.** Develop a long-term, region-wide strategy for cybersecurity that includes timelines, funding sources, and performance indicators. This roadmap should align with EU accession goals, highlighting key initiatives for regional integration in cybersecurity.

- **Establish capacity-building programmes.** Increase funding for regional capacity-building programmes to improve technical skills, leadership, and governance in cybersecurity. Programmes should include training for public officials, law enforcement, and the private sector on cybersecurity best practices.

- **Enhance public awareness campaigns.** Develop regionally coordinated public awareness campaigns to promote cybersecurity knowledge amongst citizens. This can reduce risks from phishing, misinformation, and social engineering, creating a more cyber-resilient population.

- **Enforcement of GDPR regulations and policies** in public institutions across the Western Balkans. This is crucial, as these institutions serve as the region's largest data controllers and handle vast amounts of sensitive citizen information. Enhanced compliance will not only improve data privacy and security but also build public trust and align the region with EU data protection standards, facilitating further integration and cooperation.

- **Develop a comprehensive HR strategy focused on talent sharing and retention within cybersecurity across the Western Balkans to address skill shortages and strengthen regional cyber resilience.** By fostering talent sharing and retention, the region can build a robust cybersecurity workforce, reducing dependency on external expertise and enhancing local capabilities. This collaborative approach will also create a supportive environment for career development, encouraging professionals to stay within the region and contribute to long-term cyber resilience and innovation.

good.
better.
regional.

@rccint

@regionalcooperationcouncil_rcc

@RegionalCooperationCouncil

@regionalcooperationcouncil

@RCCSec

@rcc.int

Powered by RCC.int