

UNDERSTANDING THE MEANING AND IMPACT OF THE WESTERN BALKANS' ENGAGEMENT WITH THE UN CYBERCRIME CONVENTION

Antigona Aljilji Salaj

Centre for Human Rights - Tetovo, North Macedonia, alili.antigona@gmail.com

Blerim Salihi

Centre for Human Rights - Tetovo, North Macedonia, sblerim@outlook.com

Abstract: The engagement of the Western Balkans with the United Nations Convention against Cybercrime reflects a decisive shift in the region's approach to cyber-dependent and cyber-enabled criminality within an increasingly volatile and securitized digital environment. Escalating state-sponsored cyberattacks, the growing sophistication of transnational organized cybercrime, and the use of cyber operations as instruments of hybrid warfare have exposed deep-seated structural vulnerabilities in national digital governance systems. These developments have intensified reliance on multilateral criminal justice frameworks capable of responding to cross-border threats that transcend traditional jurisdictional boundaries. Within this context, the Convention operates not only as a normative legal reference point but also as a catalyst for institutional, procedural, and strategic transformation across the region.

The paper situates the Convention within evolving regional cybercrime governance frameworks, examining its influence on the harmonization of substantive criminal law, the standardization of procedural powers related to electronic evidence, and the institutionalization of international cooperation mechanisms. Particular emphasis is placed on the regulation of investigative measures such as expedited data preservation, production orders, and real-time collection of traffic data, which collectively redefine the operational capacities of law enforcement and judicial authorities. At the same time, the Convention's conditionality framework embeds human rights safeguards – most notably proportionality, necessity, judicial authorization, and data protection – within cybercrime investigations, reinforcing the primacy of the rule of law in technologically mediated enforcement.

Despite measurable progress in legal alignment, persistent challenges continue to shape implementation across the Western Balkans. These include reactive policy development driven by crisis response, uneven institutional and technical capacity, limited inter-agency coordination, and enduring discrepancies between formal legal compliance and operational effectiveness. Cross-border criminal dynamics further complicate enforcement, underscoring the need for sustained regional trust and information-sharing. Engagement with the Convention is therefore examined alongside broader European Union integration trajectories, particularly its relevance to rule of law reforms under Chapters 23 and 24 and alignment with EU cybersecurity and data protection standards.

Ultimately, engagement with the UN Convention against Cybercrime offers a critical framework for strengthening legal coherence, enhancing regional cooperation, and advancing rights-based cybercrime enforcement in the Western Balkans. Its long-term transformative impact, however, remains contingent upon sustained political commitment, institutional transparency, judicial independence, and targeted capacity-building at both national and regional levels.

Keywords: cybercrime, Western Balkans, United Nations Convention against Cybercrime, security.

1. INTRODUCTION

Cybercrime has become one of the most complex and pervasive challenges facing contemporary criminal justice systems. The rapid expansion of digital technologies has facilitated new forms of cyber-dependent crime while simultaneously transforming traditional organized crime into increasingly cyber-enabled activities. These developments have exposed persistent gaps in domestic legal frameworks and international cooperation mechanisms, particularly in regions characterized by intense cross-border interaction and evolving institutional capacities.

In response to these challenges, the international community has sought to develop a comprehensive global legal framework to address cybercrime. The adoption of the United Nations Convention against Cybercrime represents a landmark effort to harmonize criminalization, strengthen international cooperation, facilitate access to electronic evidence, and ensure respect for human rights in cybercrime investigations. (United Nations General Assembly, 2024). For the Western Balkans, a region marked by ongoing rule-of-law reforms and European integration processes, engagement with this Convention carries distinct legal, political, and practical significance.

This paper examines the meaning and impact of the Western Balkans' engagement with the Cybercrime Convention. It argues that such engagement constitutes a strategic commitment that goes beyond symbolic alignment, reflecting a deliberate effort to enhance regional cooperation, modernize criminal justice systems, and address cyber-enabled crime in a manner consistent with international standards and human rights obligations.

2. THE CYBERCRIME CONVENTION: FRAMEWORK AND OBJECTIVES

The Cybercrime Convention was negotiated under the auspices of the United Nations General Assembly, with substantive support from the United Nations Office on Drugs and Crime (UNODC). (United Nations General Assembly, 2024; United Nations Office on Drugs and Crime [UNODC], 2023). Its development was driven by the recognition that existing regional instruments, while effective within their scope, did not offer a universally accepted framework capable of addressing the global nature of cybercrime. (Council of Europe, 2001; United Nations General Assembly, 2024).

The Convention pursues several core objectives. First, it seeks to promote the criminalization of cyber-dependent offenses, including illegal access to computer systems, data and system interference, and the misuse of devices. Second, it acknowledges the growing role of information and communication technologies in facilitating traditional crimes such as fraud, online sexual exploitation, and certain forms of trafficking in persons. Third, it establishes a framework for international cooperation tailored to the specific challenges posed by electronic evidence, including data preservation and cross-border assistance. (UNODC, 2023; United Nations General Assembly, 2024).

A defining feature of the Convention is its emphasis on safeguards. Provisions throughout the instrument underline the principles of legality, necessity, proportionality, and judicial oversight, reflecting concerns about potential overreach and misuse of cybercrime laws. (United Nations General Assembly, 2024).

3. CYBERCRIME IN THE WESTERN BALKANS: REGIONAL CONTEXT

The Western Balkans have experienced a notable increase in cyber threats and cybercrime incidents in recent years, reflecting both global digitalization trends and region-specific vulnerabilities. As public administrations, financial institutions, and everyday social interactions increasingly rely on digital technologies, criminal actors have expanded their activities to exploit online environments. Reports indicate a increasing occurrence of phishing schemes, online fraud, ransomware attacks, and intrusions targeting both public and private sector entities. (Balkan Insight, 2025; Global Initiative Against Transnational Organized Crime, 2024).

Geopolitical developments have further intensified cyber risks in the region. Following heightened international tensions, cyberattacks against Western Balkan countries appear to have grown in both frequency and sophistication, targeting critical services and undermining public trust. (Balkan Insight, 2025). At the same time, cybercrime in the region often intersects with traditional organized crime. Long-established criminal networks active in trafficking, smuggling, and financial crime increasingly rely on digital tools for recruitment, coordination, and concealment of illicit proceeds. (Global Initiative Against Transnational Organized Crime, 2024).

Institutional capacity to investigate and prosecute cybercrime remains uneven across the Western Balkans. While most states have adopted cybersecurity strategies and criminalized core cyber offenses, practical challenges persist, including limited technical expertise, investigative units with limited resources, limited digital forensic capacity, and limited cooperation with private service providers. (DCAF, 2021; Metamorphosis Foundation, 2022). Reporting and prosecution rates remain low in several jurisdictions, highlighting gaps between legal frameworks and operational effectiveness. (Metamorphosis Foundation, 2022)

In parallel, Western Balkan states are undergoing broader rule-of-law reforms linked to European integration processes. Alignment with international standards on criminal justice, data protection, and fundamental rights remains a priority. (European Commission, 2023). Within this context, engagement with global legal instruments on cybercrime responds not only to security concerns but also to strategic objectives of legal harmonization, regional cooperation, and institutional credibility.

A regional risk bulletin similarly warns that "the lack of preventative measures has left South Eastern Europe at an increased risk of cyber-enabled crime" (Global Initiative Against Transnational Organized Crime, 2024, p. 1).

As one regional review notes, "providing for inclusive, transparent and responsive cooperation amongst public and private sectors, academia, and civil society" (DCAF, 2021, p. 1).

4. MEANING AND IMPACT OF ENGAGEMENT WITH THE UN CONVENTION AGAINST CYBERCRIME

The engagement of Western Balkan countries with the United Nations Convention against Cybercrime marks a critical transition from reactive national defenses to participation in a global criminal justice policy (UNODC, 2023; United Nations General Assembly, 2024). As the region faces an escalation in state-sponsored cyber operations and hybrid warfare - exemplified by destructive attacks against infrastructure in Albania, Montenegro, and Kosovo - this engagement serves as an essential framework for regional security and European Union (EU) integration (BIRN, 2025).

For Western Balkan economies, engagement with the UN Convention means committing to a standardized, comprehensive international legal framework. This requires the criminalization of specific digital acts, including illegal access to systems, illegal interception of transmissions, and data or system interference.

Engagement also mandates the adoption of procedural powers to facilitate investigations. These include the expedited preservation of stored electronic data for up to 90 days, production orders for subscriber information, and the real-time collection of traffic data. Furthermore, it provides the legal basis for international cooperation, such as the sharing of electronic evidence for serious crimes and participation in a 24/7 network for immediate investigative assistance. (UNODC, 2023; United Nations General Assembly, 2024).

The primary impact of this engagement is visible in the acceleration of institutional development across the region.

Kosovo has moved to establish its Cyber Security Agency (CSA) and launched the State Training Centre for Cyber Security in 2024 to provide specialized education for public officials. (BIRN, 2025)

Montenegro adopted a decision in late 2024 to establish an Agency for National Security to centralize cyber expertise, while simultaneously aligning its legislation with the EU's NIS2 Directive. (BIRN, 2025)

Albania has demonstrated significant sector-specific advancement, with the banking sector achieving a 94% adoption rate of cybersecurity measures following recent reforms. (BIRN, 2025)

Strategically, engagement impacts EU accession negotiations, particularly regarding Chapters 23 and 24. The Regional Cooperation Council (RCC) facilitates this by supporting the alignment of WB legislation with the EU acquis and building the capacity of national CSIRTs. However, much of this progress remains reactive, occurring in the aftermath of large-scale attacks rather than through proactive planning. (BIRN, 2025)

5. HUMAN RIGHTS CONSIDERATIONS AND SAFEGUARDS

Crucially, the UN Convention mandates that the implementation of investigative powers must be consistent with international human rights law. Under Article 24, WB countries must ensure that all procedural measures incorporate the principle of proportionality and are subject to judicial or independent review (UNODC, 2023; United Nations General Assembly, 2024).

Privacy and Data Protection: Investigative measures are often more intrusive than traditional "offline" searches because digital devices collect unprecedented volumes of personal data. (OSCE, 2023) States must ensure personal data is received subject to effective safeguards to prevent arbitrary or unlawful interference with privacy (UNODC, 2023; United Nations General Assembly, 2024).

Freedom of Expression: There are growing concerns that cybercrime laws could be used as tools for censorship. For example, new legislation in the wider region that criminalizes the creation of a "false perception" of a data leak has been criticized for its potential to suppress independent journalism (BIRN, 2025).

State Repression: Reports from Serbia have highlighted the use of invasive spyware and digital forensic tools by authorities to monitor activists and journalists, reflecting a broader trend of state-led repression that conflicts with the Convention's human rights obligations. (BIRN, 2025)

Transparency: A lack of institutional transparency regarding data breaches persists, with some WB authorities failing to disclose leaks even after sensitive data appeared for sale on the dark web. (BIRN, 2025)

Ultimately, while the Convention provides the legal tools to combat high-tech crime, the Western Balkans must balance these powers with democratic values to ensure that the drive for security does not erode the digital rights of its citizens.

6. CONCLUSION

Engagement with the United Nations Convention against Cybercrime marks a structural turning point in the Western Balkans' approach to digital security, criminal justice, and international legal cooperation. It reflects a shift from fragmented and reactive national responses toward participation in a harmonized global framework designed to address cyber-dependent and cyber-enabled crime. In a region characterized by rapid digitalization, geopolitical volatility, and evolving rule-of-law reforms, the Convention functions as both a legal instrument and a catalyst for institutional modernization.

Its influence is visible in the alignment of domestic criminal legislation, the expansion of procedural powers for handling electronic evidence, and the strengthening of international cooperation mechanisms, including 24/7 points of contact and cross-border data exchange. Engagement with the Convention also intersects directly with EU accession trajectories, particularly under Chapters 23 and 24, reinforcing legal harmonization, cybersecurity governance, and accountability standards. However, implementation across the region remains uneven. Progress is frequently reactive, triggered by major cyber incidents rather than sustained strategic planning, and is constrained by shortages of technical expertise, limited digital forensic capacity, and gaps in inter-agency coordination.

Most critically, the Convention embeds the fight against cybercrime within a rule-of-law framework that conditions investigative powers on legality, necessity, proportionality, and judicial oversight. This safeguard architecture is essential in a regional context where concerns persist regarding surveillance overreach, misuse of cybercrime laws for political control, and insufficient data-protection guarantees. The long-term legitimacy of cybercrime enforcement in the Western Balkans will therefore depend not only on legal compliance, but on transparent institutions, independent judicial review, and meaningful protection of fundamental rights.

Ultimately, the Convention provides the Western Balkans with a coherent legal and cooperative foundation to strengthen cyber resilience and confront transnational digital threats. Its transformative potential, however, will be realized only if states move beyond formal alignment toward genuine operational capacity, proactive policy development, and a sustained commitment to democratic governance in the digital sphere.

REFERENCES

- Council of Europe. (2001). *Convention on Cybercrime (Budapest Convention) (CETS No. 185)*. European Treaty Series No. 185.
- DCAF – Geneva Centre for Security Sector Governance. (2021). *National cybersecurity strategies in Western Balkan economies*.
- Elshani, D. (2025). *Navigating the evolving threat landscape and institutional responses to cybersecurity threats in the Western Balkans*. Balkan Investigative Reporting Network (BIRN)
- European Commission. (2025). *Communication on EU Enlargement Policy*. COM (2025) 690 final.
- European Commission. (2025). *State of play: EU accession negotiations*.
- Global Initiative Against Transnational Organized Crime. (2024). *Cyber-enabled crime poses significant risks to South Eastern Europe (Risk Bulletin No. 19)*.
- Metamorphosis Foundation. (2022). *A recent look towards cybersecurity in the Western Balkans: How can we improve the cybersecurity level in the region? (ICEDA Project)*.
- Rakha, N. A. (2024). Cybercrime and the law: Addressing the challenges of digital forensics in criminal investigations. *Mexican Law Review*, 16(2).
- OSCE Secretariat, Transnational Threats Department. (2023). *Ensuring human rights compliance in cybercrime investigations: OSCE training guide for criminal justice practitioners*.
- Regional Cooperation Council. (2023). *Eighth Regional (Jumbo) Security Coordination Conference: Security cooperation in the Western Balkans – Securing the future: Building resilience through collaboration*.
- Tafa, I., & Vrajolli, M. (2025). *Why the EU must integrate the Western Balkans into its cybersecurity agency? European Western Balkans*.
- United Nations General Assembly. (2024). *Resolution 79/243: United Nations Convention against Cybercrime; Strengthening international cooperation for combating certain crimes committed by means of information and communications technology systems and for the sharing of evidence in electronic form of serious crimes*.
- United Nations Office on Drugs and Crime. (2023). *Cybercrime and electronic evidence: Legal and practical considerations*.