Maria João Guia

Research and Knowledge Management Officer, Editor-in-Chief

https://doi.org/10.3013/dxmpxz16

This editorial foreword introduces the seventh issue of the conference bulletin of the *European Law Enforcement Research Bulletin* (Bulletin), marking a further milestone in a series dedicated to advancing rigorous, practice-oriented scholarship on police science, contemporary crime and security challenges. This issue draws on the proceedings of the 2024/2025 Research & Science Conference held in March 2025 in Ostia (Italy), devoted to the analysis of high-risk criminal networks (HRCNs). The Bulletin continues its core mission: to provide a credible forum where empirical research, theoretical development and operational insight intersect, offering value to scholars, practitioners and policy communities alike.

The conference proved to be a substantive and timely success. Bringing together researchers, policymakers, EU officials, analysts and law enforcement professionals from diverse jurisdictions, it nurtured sustained dialogue on the structure, resilience and adaptive capacity of HRCNs. Contributions addressed methodological innovation, cross-border cooperation and the implications of technological change for both criminal organisation and investigative response. The quality and diversity of the exchanges confirmed the relevance of the conference series as a stable platform for informed, evidence-based debate.

As Editor-in-Chief and, together with the Editorial Board members, I remain committed to maintaining the Bulletin's academic integrity, editorial independence and relevance to applied research. This role entails not only coordinating and reviewing contributions of the highest scholarly standard, but also ensuring coherence across disciplines and perspectives represented in each issue. The present volume reflects that commitment, offering carefully selected papers that combine analytical depth with operational relevance and that collectively advance understanding in this complex field.

This issue would not have been possible without the sustained dedication of the Editorial Board members and the editors' assistants, whose expertise, diligence and commitment continue to set a high benchmark for the publication.

I also extend my sincere appreciation to the authors for their rigorous and original contributions, and to the reviewers for their thorough, constructive and timely assessments. Their collective efforts underpin the scientific quality of this bulletin and reinforce its standing as a trusted reference within the law enforcement research community.

In the pages that follow, each chapter is introduced through a concise analytical synopsis designed to guide the reader through its core arguments, methodological approach and principal findings. These summaries are intended not merely as descriptive short abstracts, but as structured points of entry that situate each contribution within the broader thematic framework of HRCNs addressed in this issue. By foregrounding conceptual focus and empirical relevance, the chapter synopses aim to facilitate an informed and coherent reading of the volume as a whole, while allowing readers to identify points of convergence, complementarity and critical dialogue across contributions.

The opening article, awarded the best paper recognition, authored by Patricia Faraldo Cabana, offers a rigorous and critical examination of how the European Union has progressively framed the trafficking of cultural goods as a form of organised crime within its policy architecture. Drawing on a systematic qualitative content analysis of EU policy documents published between 1993 and 2023, the article traces the historical emergence, consolidation and transformation of this narrative, with particular attention to its increasing association with terrorism, terrorist financing and money laundering. The author demonstrates that, despite the growing policy emphasis on these links, EU approaches remain conceptually fragile and often rely on unsubstantiated assumptions regarding the organised and transnational nature of cultural property crime. The article persuasively argues that this lack of conceptual clarity risks generating misguided policy responses, while also identifying a significant policy shift of potential value: the incorporation of art market actors into the EU anti-money-laundering (AML) framework. By situating trafficking in cultural goods at the intersection of organised crime control, white-collar crime regulation and cultural heritage protection, the contribution provides an empirically grounded and theoretically informed critique that sets a strong analytical tone for the volume.

Gabriela Boneva, Luke Bates and Babak Akhgar authored the second chapter. In short, it maps the current EU landscape of new psychoactive substances (NPS) as a rapidly evolving drug phenomenon that strains both public health systems and law enforcement capacity. The article explains how NPS markets exploit legal fragmentation and chemical 'micro-innovation', producing substances that mimic controlled drugs while remaining difficult to schedule, identify and detect. Building on a two-stage design – an extensive review of academic and official sources complemented by structured consultations with practitioners from law enforcement agencies and postal services involved in the ARIEN project – the chapter reconstructs how NPS circulate through hybrid online–offline supply chains, frequently using Surface Web and Dark Web retail and relying heavily on postal and courier logistics. Boneva et al. synthesise evidence on prevalence (notably synthetic cathinones and synthetic cannabinoids), concealment and distribution tactics (including prison-focused methods such as paper impregnation), and the broader risk environment shaped by inconsistent forensic tools, limited automated online investigative capabilities and patchwork national control models (generic, substance-by-substance or hybrid). The chapter closes by identifying concrete capability gaps – particularly in detection technologies, cross-border intelligence integration and legislative harmonisation – and proposes a forward agenda that aligns regulatory coordination with operational realities and the escalating health harms associated with unknown potency and polysubstance exposure.

The third contribution, produced by Aleksandar Atanasov, provides an in-depth, operationally grounded analysis of HRCNs involved in migrant smuggling in Bulgaria, examined through criminological, law enforcement and intelligence lenses. Focusing on developments observed over the last three years, the chapter reconstructs the organisational logic and modus operandi of these networks by integrating open-source materials with analytically framed professional insight. Central to the analysis is the identification of five interrelated drivers – geosocial, local, foreign, criminal and non-criminal, and geopolitical factors – that together shape the structure, adaptability and resilience of smuggling networks operating along the Western Balkan and Eastern Mediterranean routes. The study details how Bulgarian-based criminal infrastructures interact with foreign facilitators, exploit challenging border terrain, deploy layered transport tactics and rely on a differentiated division of labour ranging from drivers and guides to field captains and network leaders. Beyond operational patterns, the chapter situates migrant smuggling within a broader security context, highlighting points of convergence with corruption, poly-criminality and, in specific cases, terrorism-related risks. By systematically mapping roles, routes and enabling environments, the article offers policy-relevant insights into how these networks function as service-oriented criminal enterprises and underscores the need for integrated, cross-border responses that address both immediate operational threats and the wider structural conditions sustaining them.

In Article 4, Hanna-Mari Lahtinen and five colleagues tackle a central problem in combating online child sexual abuse and exploitation: the evidential and behavioural 'blind spot' created by the fact that most child sexual abuse material (CSAM) users are never detected. Rather than relying on clinical or forensic cohorts, the authors describe and evaluate a replicable Dark Web data collection model that intercepts CSAM-related search activity on a Tor search engine and redirects users to an anonymous, multi-language survey alongside links to support services. Using responses from a large pool of self-identified CSAM searchers (with a final analytic sample exceeding 2 000 after exclusions), the study compares three self-reported groups – those reporting prior charges for sexual crimes against children, those reporting charges against adults and those reporting no charges – across motivational, behavioural and situational indicators. The findings underline meaningful heterogeneity within this offending population: variables such as prior violent charges, seeking material depicting the abuse of very young children, grooming behaviours and physical contact with children are associated with elevated likelihood of belonging to the 'charged' groups, while a substantial subgroup reports no charges and appears more receptive to preventive engagement. The chapter's contribution is therefore twofold: it demonstrates a practical method for accessing otherwise hidden offender data at scale, and it translates the resulting risk-relevant patterns into implications for law enforcement and prevention – particularly the value of integrating CSAM screening into wider sexual and violent crime investigations and of using online 'choice points' (search interfaces) to divert users toward disruption and help pathways.

The following article is authored by Victoria Koutsoupia, and it examines how confiscation, whistleblowing and technological innovation can be combined to disrupt the structural resilience of HRCNs across the EU. Rather than approaching organised crime solely through prosecution, the article reframes the problem as an economic and systemic one, arguing that criminal networks are most effectively weakened by depriving them of illicit profits and informational advantages. Through a qualitative, multi-method analysis of EU legislation, policy instruments and selected case studies, the chapter shows how asset confiscation targets the financial core of organised crime, while whistleblowing functions as a critical catalyst for detection and evidentiary development – particularly in complex, transnational cases. The analysis situates these tools within an increasingly digital criminal environment, where

encryption, crypto-assets and online platforms both facilitate criminal activity and open new avenues for enforcement through blockchain analytics, interoperable databases and secure reporting technologies. By assessing recent legal developments such as Directive 2024/1260 ([1]) and EU whistleblower protection frameworks alongside technological enforcement practices, the article demonstrates that no single instrument is sufficient in isolation. Its central contribution lies in articulating an integrated strategy in which confiscation, protected insider reporting and advanced technologies operate synergistically, offering a policy-relevant roadmap for dismantling HRCNs while safeguarding fundamental rights and reinforcing cross-border cooperation.

Article 6, written by Mari-Liis Tohvelmann and co-authored by three other authors, evaluates whether a serious-game, avatar-based training tool for investigative interviewing (with adult witness avatars) produces skills that generalise beyond the simulated setting to interviews with human witnesses. Using a pre-registered, between-groups experiment with 58 novice interviewers (feedback versus no-feedback control), participants completed four avatar interviews followed by a live online interview with a mock adult witness who had viewed a short crime video about a week earlier. The study operationalises interview quality through a widely used distinction between recommended question types (free recall, cued recall, open questions) and non-recommended types (closed, forced-choice, suggestive, misleading), and further examines whether questioning style translates into more accurate witness accounts. Results indicate that process feedback during avatar practice reliably reduced non-recommended questioning styles and increased the proportion of recommended questions during training; crucially, this pattern transferred to the subsequent mock-witness interview, where the feedback group again used fewer non-recommended questions and a higher recommended-question proportion. However, the intervention did not yield measurable gains in the amount or proportion of correct details elicited from the mock witnesses, suggesting that the improving question form alone may be insufficient – at least for novices, brief training doses, short stimulus events and relatively high baseline adult accuracy. The authors interpret these findings as evidence that avatar training with immediate feedback can shift interviewer behaviour in a direction consistent with best-practice guidelines, while also highlighting the need for future work (e.g. modelling components, AI-assisted coding, practitioner samples and designs that better test evidential yields) to translate improved interviewing style into consistently better investigative outcomes.

Denis Solodov is the author of Article 7, which examines how Poland's approach to cooperating witnesses in organised crime cases can be strengthened through the adoption of the UN Méndez Principles on Effective Interviewing. It argues that while cooperating witnesses are often crucial sources of insider evidence, their testimony is inherently exposed to bias, strategic self-interest and procedural vulnerabilities, particularly given incentive structures such as leniency or immunity and shifts in procedural status. By analysing Polish witness categories and recurring practical challenges – including corroboration deficits, limited defence participation and the sophistication of organised-crime actors – the chapter shows how traditional, confirmatory interviewing practices and reliance on written protocols may undermine evidential reliability. It concludes that integrating non-coercive, rapport-based interviewing, supported by mandatory audiovisual recording, targeted training and clearer procedural safeguards, would enhance both the quality of evidence and the legitimacy of organised crime investigations.

([1]) Directive (EU) 2024/1260 of the European Parliament and of the Council of 24 April 2024 on asset recovery and confiscation, OJ L, 2024/1260, 2.5.2024, ELI: http://data.europa.eu/eli/dir/2024/1260/oj.

Article 8, authored by Zaur Gouliev, conceptualises 'disinformation as a service' as a maturing form of organised cybercrime in which influence operations are commodified, modular and sold to state and non-state clients through the same market logic that underpins crime-as-a-service ecosystems. Drawing on a case study of the 'Doppelganger' campaign, a systematic review of Surface Web and Dark Web marketplaces and a macro-analysis of foreign information manipulation around elections, the article shows how cloned media sites, automated amplification, ad-tech tools and bulletproof hosting are combined into resilient influence pipelines. These capabilities are traded alongside malware and access brokerage, evidencing a convergence between disinformation and cybercrime that lowers barriers to entry, frustrates attribution and enables rapid reconstitution after takedowns. The study concludes that disinformation as a service represents an HRCN model whose disruption requires law enforcement responses that target both market supply chains and campaign infrastructure through coordinated, cross-border and technologically integrated strategies.

Luna Filipović is the author of Article 9. She demonstrates how forensic linguistics can materially strengthen the investigation of international and organised crime by improving both evidence elicitation and intelligence analysis in multilingual contexts. Drawing on a large body of authentic police–suspect interactions from the United Kingdom and the United States, the chapter shows how questioning style, translation practices and unexamined linguistic and cultural assumptions can generate miscommunication, distort meaning and weaken evidential value – particularly in cross-language interviews. Beyond face-to-face policing, the article extends forensic linguistic insight to Dark Web communications, illustrating how systematic features of non-native English can reveal offenders' linguistic backgrounds and collaborative patterns within transnational criminal networks. By integrating empirical linguistic research, applied language typology and real investigative data, the chapter argues that forensic linguistics remains an underused yet scientifically robust resource for law enforcement, offering concrete benefits for accuracy, fairness and effectiveness in complex, multilingual criminal investigations.

Article 10, written by Pasquale Danese, argues that VAT (value added tax) fraud and false invoicing have become central mechanisms through which organised crime now generates and launders proceeds inside the legal economy, forcing a rethink of the classic 'placement–layering–integration' model. Building on European and Italian threat reporting, the chapter proposes that laundering dynamics vary systematically with the type and sophistication of criminal activity: low-complexity predatory crime still yields cash and fits the traditional model, whereas financial-crime networks increasingly produce 'already-banked' illicit revenues (and cybercriminal groups produce crypto-denominated proceeds), making 'placement' less decisive and shifting the operational problem toward separating funds from their origin under high traceability conditions. To capture this transition, the author introduces an AI-assisted 'declining sigmoid' function linking criminal sophistication to the share of cash proceeds, and advances a new phase – 'dissociation' – to describe strategies such as cross-border transfers to non-cooperative jurisdictions, monetisation/cash-out through intermediaries and crypto-based obfuscation (e.g. mixers, chain-hopping, DeFi (decentralised finance) mechanisms). The core contribution is a three-level framework (cash, traditional finance, DeFi/crypto) that treats laundering as context-dependent rather than linear, with implications for investigative training, asset tracing and EU cooperation against financially embedded criminal networks.

We then find Murat Tina's Article 11, which examines how foreign terrorist fighters (and returnees) intensify the convergence between organised crime and terrorism, arguing that recent conflict dynamics – especially those linked to Syria and broader governance collapse in the Levant – have accelerated a shift from occasional, transactional

cooperation to more durable, mutually reinforcing relationships. Drawing on desk-based analysis of scholarship, policy reporting and open-source data, the chapter traces how terrorist groups increasingly adopt profit-driven criminal practices (smuggling, trafficking, document fraud and money laundering), while criminal networks benefit from the operational reach, skills and ideological cover that foreign terrorist organisations can provide. The author treats foreign terrorist fighters as 'bridging actors' who move between milieus, connect local illicit markets to transnational extremist infrastructures and help standardise shared methods (routes, facilitators, informal finance, crypto channels), with illustrative discussion of patterns linked to the Islamic State in Iraq and Syria (ISIS) and the Kurdistan Workers' Party (PKK). The main implication is strategic: threat assessment and enforcement models that rigidly separate 'crime' from 'terrorism' understate hybrid risk, so responses should integrate cross-border intelligence, financial disruption, database interoperability and prevention measures (including prison-focused de-radicalisation and post-return monitoring) to target the combined ecosystem rather than its components in isolation.

Article 12, authored by Wendy Schreurs and two co-authors, argues that Dutch efforts against HRCNs are increasingly shaped by data-driven policing built around the operational exploitation of digital traces – especially encrypted communications once lawfully accessed – while stressing that technical capability alone is insufficient without organisational and ethical governance. Using interviews with strategic actors in the Dutch National Police, the authors describe how decrypted datasets from platforms such as EncroChat / Sky ECC / ANOM can produce actionable intelligence and arrests, but only when fused with other sources (e.g. automatic number plate recognition, open-source intelligence, video, seized devices) and translated into interventions through multidisciplinary work. The analysis frames data-driven policing as an evolution of intelligence-led policing, operationalised through models that integrate behavioural, technical and quantitative layers (e.g. the collect, store, analyse, engage – CSAE – model), yet repeatedly highlights 'human-in-the-loop' necessities: contextual interpretation, professional discretion and leadership that can bridge analysts and investigators. Implementation barriers are mapped across four domains – outdated ICT and storage, data quality and bias ('garbage in, garbage out'), cultural reluctance to share information and the legal–ethical friction created by surveillance technologies and opaque algorithms – leading to a central conclusion that effectiveness against adaptive HRCNs depends on sustained investment in infrastructure, skills, flexible team structures, clear authorisation/oversight mechanisms and continuous ethical review alongside technical innovation.

Article 13 is written by Jasmin Saarijärvi and nine co-authors, and it synthesises findings from the EU-funded Poseidon project, mainly on how corruption operates as an enabling condition for organised crime within EU seaport supply chains, especially in containerised trade. Drawing on desk research, interviews, focus groups, surveys and six case studies (Rotterdam, Antwerp-Bruges, Piraeus, Algeciras, Cartagena and Venice), the study maps where and why ports become vulnerable: high-throughput logistics, time-sensitive cargo (notably perishables) and complex documentation workflows create pressure points that organised crime groups exploit through bribery, information leakage and manipulation of inspections. The analysis distinguishes step-specific risks (e.g. 'rip-on/rip-off' insertion in terminals, compromised customs risk-selection, PIN-code abuse for container pickup, corruption of transporters and ship personnel) from structural drivers that cut across the chain, such as extensive human involvement in key tasks, uneven digitalisation and access controls, close-knit port labour communities, procurement and political exposure and friction in public–private information-sharing under legal constraints. Poseidon identifies early countermeasures – digitalisation, integrity screening, training and awareness and stronger public–private cooperation – while building an EU stakeholder network and an interactive dashboard to support transferability

assessment and, ultimately, make recommendations toward an EU port supply chain integrity standard, emphasising that effective responses must be tailored to port-specific conditions yet coordinated at the EU level to reduce displacement ('waterbed') effects.

Article 14 is presented by Halima Guelai, continuing the seaport topic as it examines how anti-corruption policy in the Port of Antwerp-Bruges has evolved alongside surging cocaine flows, violence and insider-enabled infiltration, arguing that corruption should be treated not simply as a facilitating factor but as a constitutive element of organised drug crime within port ecosystems. Using a 2013 port assessment, a targeted literature review (2013–2025) and 23 expert interviews, the study evaluates measures introduced over the last decade through five governance pillars – role clarity in multidisciplinary cooperation, political backing, evidence-based design, long-term orientation and adaptive capacity – and finds a persistent tilt toward 'visible' deterrence (screening, port bans, surveillance and access-control technologies) rather than the social, administrative and political conditions that sustain corrupt opportunity structures. It shows how fragmented mandates across police, customs, prosecutors, port authorities and private operators – combined with capacity constraints, legal barriers to information sharing, reliance on temporary labour and shifting modus operandi revealed by cases like Sky ECC – limit proactive prevention and encourage displacement rather than durable risk reduction. Technological fixes such as blockchain-based container pickup can harden specific vulnerabilities, but the article stresses that they may relocate pressure onto other roles unless these fixes are embedded in integrity governance, cybersecurity, reporting protections (e.g. PortWatch), sustained training and organisational change. The recommended trajectory is an integrity-based strategy grounded in shared responsibility, trust and continuous monitoring – accepting that 'zero corruption' is neither realistic nor efficiency-neutral – while pointing to policy windows such as Belgium's push to expand the International Ship and Port Facility Security Code and the coordinating potential of a national drugs agency to move from episodic securitisation toward a more integrated, evaluable and resilient anti-corruption architecture.

Kristin Weber is the author of Article 15 and she argues that social network analysis (SNA) – when anchored in legally validated evidence – can materially strengthen counterterrorism investigations by converting fragmented case material into an interpretable map of covert, high-risk networks. Drawing on 36 final court cases (2014–2017) involving ISIS-linked offences in Germany (excluding Al-Qaeda), the study combines qualitative file coding with SNA to reconstruct a network of 255 individuals and 650+ ties, distinguishing roles such as recruiters, preachers, propagandists, facilitators and foreign terrorist fighters. Using Gephi visualisation and standard centrality measures (degree, betweenness, closeness), the analysis shows how operational capacity depends not only on visible leaders but also on brokers and bridging nodes that connect peripheral clusters to core actors and sustain information, resource and mobilisation flows. A detailed subnetwork example (SR49–SR52) illustrates how a small set of peripheral yet well-positioned recruiters – reinforced by kinship ties – can drive departures to conflict zones and maintain linkage to a central preacher node, implying that targeted disruption of such connectors could fragment network functionality and prevent recruitment cascades. The article concludes that SNA is most valuable as a police training and investigative decision-support tool – improving risk assessment, prioritisation and inter-agency coordination – while warning that network adaptation, data incompleteness and overreliance on first-degree ties require longitudinal monitoring and higher-order network perspectives to detect reconfiguration after interventions and to anticipate renewed mobilisation.

Marco Garofalo and colleagues present Article 16, reporting on a European multidisciplinary platform against criminal threats (Empact) HRCN operational action led by Italy's Central Operations Service, which pilots a prevention-oriented methodology to index the risk of Italian mafia infiltration in foreign economies by shifting attention from classic 'sentinel crimes' toward business, ownership and contextual indicators that signal reinvestment, market distortion and corrupt access to procurement or regulated sectors. Built through collaboration among the State Police, Guardia di Finanza, Direzione Investigativa Antimafia, the European Union Agency for Law Enforcement Cooperation (Europol) and the Università Cattolica del Sacro Cuore of Milan's Transcrime research centre, the project operationalises Italy's anti-mafia experience (including the organisational logic associated with Article 416-bis) into a two-track assessment: (i) investigative profiling of managers / beneficial owners using structured intelligence and open-source criteria (relationships, judicial history, professional/financial traces), and (ii) a data-driven corporate risk model derived from Orbis data that compresses hundreds of candidate variables into a calibrated set of indicators spanning ownership opacity, territorial clustering, anomalous officer profiles, financial irregularities, adverse events and political exposure. From 59 nominated firms across catering, earth-moving/construction and gaming/betting, Transcrime could reliably identify 42 and classified most as high risk, highlighting patterns such as complex multilayer ownership, shareholders just below beneficial ownership disclosure thresholds, unusually elderly beneficial owners, high co-location of firms at the same address and creditor-payment anomalies – features that are more prevalent than in a matched control group. The combined analyses suggest that infiltration risk concentrates differently by sector and geography, that low-profile sectors may function as quieter vehicles for reinvestment and that convergence between policing assessments (including links to suspicious transaction reports and prior mafia-related records) and statistical scoring can improve targeting; the paper's core implication is that stable cross-border information exchange and shared analytical standards are necessary to turn such hybrid, indicator-based scoring into a durable tool for early detection and coordinated disruption of mafia economic penetration abroad.

The authors of Article 17, Ana Isabel Barros and colleagues, then argue that illicit markets should be analysed as adaptive 'business systems' rather than only as logistics chains or social graphs, and propose an exploratory, computational approach that links a criminal organisation's value chain (financial, logistical and social) to the time-dependent effects of law enforcement interventions. Using cocaine trafficking as the illustrative domain, Barros et al. frame criminal networks as complex adaptive systems whose profit incentives, embeddedness in legitimate economies and capacity to change modus operandi generate resilience and unintended intervention effects (e.g. displacement, violence escalation, corruption). The paper operationalises 'criminal business modelling' through stakeholder / value-network analysis, business model canvas mapping and cost–benefit quantification under uncertainty, then translates these insights into an agent-based simulation designed less for prediction than for learning and strategy design. Three stylised business models (smuggling via a Dutch port, routing via an alternative EU port and 'cocaine laundry' impregnation/extraction) are parameterised with differing cost structures, and simulated policing strategies shift relative profitability by raising targeted costs (with particular sensitivity in corruption and specialised nodes). The model's core contribution is pedagogical and organisational: by visualising how focused enforcement can leave profits intact (e.g. easily replaced extractors), trigger a waterbed effect (route switching) or create rapid cycling among business models, it supports double-loop learning – forcing decision-makers to revisit assumptions, anticipate adaptation and consider sustained, system-wide interventions that reduce overall attractiveness rather than merely reallocating pressure.

Article 18, by Sónia Morgado and Sérgio Felgueiras, examines *Ozark* (Season 1) as a criminological text, using mixed-method content analysis (thematic coding plus discourse analysis, supported by frequency counts) to map how the series depicts recruitment into organised crime and how closely those portrayals align with established frameworks. The authors treat recruitment as a multi-causal process shaped by structural strain, social learning and differential association and rational choice calculations, showing how characters are drawn in through a combination of economic precarity, social and familial obligations, opportunity structures and progressive moral disengagement; recruitment is portrayed less as a single 'moment' than as an incremental entanglement where coercion, manipulation and perceived necessity recalibrate actors' cost–benefit judgements over time. The analysis also situates these depictions within scholarship on media effects, arguing that serialised crime narratives can both reflect real recruitment tactics (e.g. exploiting vulnerability, leveraging trust networks, normalising deviance) and distort public understanding via simplification, stereotyping and glamorisation, with downstream implications for attitudes toward punishment, policing and prevention. By focusing on the season that establishes core relationships and motivations, the study claims a methodologically 'clean' window into early-stage criminal immersion, and it concludes that *Ozark* offers a plausible – though dramatised – representation of recruitment dynamics that can be used pedagogically (e.g. for media literacy or practitioner training) if interpreted critically and without treating fiction as direct empirical evidence.

Jasmin Saarijärvi and Mark Worth, authors of Article 19, situate corruption in the EU's financial sector as a two-way phenomenon – where institutions can be simultaneously exploited by and complicit in illicit finance – and frame it as a priority domain within the EU's emerging anti-corruption strategy, informed by a European Commission mapping exercise that flags finance (alongside procurement, construction, healthcare, defence/security and sports) as a high-risk area requiring stronger regulation, oversight, investigation and enforcement. The authors argue that the sector's decentralisation, digitisation and sheer transactional volume create 'black holes' for monitoring, while organised crime groups leverage professional enablers (lawyers, notaries, accountants, real-estate actors) and offshore structures to build parallel criminal economies that blur upperworld/underworld boundaries and complicate attribution of responsibility. Money laundering and tax evasion are treated as the most consequential corruption-linked crimes, intertwined with fraud, sanctions / terrorism-financing risks and cyber-enabled victimisation, with low asset recovery rates and under-investigation amplifying perceived impunity; the piece further highlights operational obstacles such as divergent national predicate-offence regimes, beneficial ownership opacity (shell entities, layered structures) and the growing misuse of fintech, crypto, DeFi, virtual IBANs (international bank account numbers) and neobanks. In societal terms, the analysis links financial corruption to macro-level harms – reduced growth, weakened public trust and the reinforcement of underground governance by criminal networks – while emphasising that effective countermeasures will require closing regulatory and data gaps, improving cross-border cooperation and targeting the enabling ecosystems that reduce criminals' transaction costs and shield illicit flows from scrutiny.

The author of Article 20 is Ioannis Vlassis and he analyses why police forces and prosecution services across the six countries of the Western Balkans ([2]) continue to struggle with integrity and operational independence despite extensive EU-aligned reforms, using a comparative research design (2023–2024) that triangulates legal/institutional review, case studies and expert interviews. The core finding is that informal political leverage – exerted through

([2]) Albania, Bosnia and Herzegovina, Kosovo (*), Montenegro, North Macedonia and Serbia. (*) This designation is without prejudice to positions on status, and is in line with UNSCR 1244/1999 and the ICJ Opinion on the Kosovo declaration of independence.

appointments, disciplinary tools and opaque case allocation – interacts with organised crime influence to produce selective enforcement, downgraded or delayed sensitive investigations and persistently low public trust. The paper further shows how fragmented oversight architectures and weak coordination among internal control units, prosecutors, parliaments, ombuds bodies, civil society and international partners limit prevention and learning, while resource constraints, outdated digital infrastructure and uneven specialised skills (e.g. financial investigations, cyber-enabled evidence) reduce prosecutorial and investigative effectiveness. Illustrative cases (e.g. Albania's 2023 assault episode, North Macedonia's post-wiretapping accountability efforts, Montenegro's 2023 court-evidence 'tunnel and Serbia's Sky ECC leak case) are used to demonstrate the gap between formal compliance and practical resilience. Finally, the article treats gender imbalance as both an integrity risk and a performance issue – especially where merit-based progression is undermined – arguing that sustainable rule-of-law gains require enforceable safeguards against interference, stronger accountability mechanisms, professional capacity building and gender-sensitive leadership pathways rather than further purely technocratic legal reforms.

Article 21, authored by Alp Cenk Arslan, conceptualises high-risk cybercriminal networks as industrialised, transnational ecosystems whose resilience is reinforced by a variable 'state–cybercrime nexus' (state-operated, state-enabled, state-tolerated) and argues that this alignment increasingly sits within contemporary geopolitical security doctrines. Using qualitative comparative analysis and structured documentary coding, the study systematically contrasts the US National Cybersecurity Strategy (2023) and the EU cybersecurity strategy for the digital decade (2020) across three analytic nodes – operational disruption, regulatory resilience and diplomatic attribution – while drawing on illustrative cases linked to China, North Korea and Russia, to show how state protection, tolerance or direct tasking amplifies criminal capability. The comparative findings indicate a strategic divergence: the United States prioritises persistent engagement, cost imposition and infrastructure/finance takedowns ('defend forward'), whereas the EU emphasises harmonised governance, 'secure-by-design' obligations and cross-border preparedness to strengthen guardianship and reduce opportunity structures. In parallel, the article identifies enduring transatlantic 'grey zones' created by mismatched legal thresholds, evidentiary timelines and jurisdictional fragmentation that allow networks to reconstitute faster than institutions can coordinate attribution, seizures and prosecutions. The paper concludes by proposing an integrated response that couples advanced technologies (e.g. AI-enabled detection, readiness for quantum-era risks) with tighter public–private operational integration, interoperable legal frameworks and structured inter-agency partnerships – particularly to support EU law enforcement in evidence production, disruption coordination with the European Cybercrime Centre within Europol and sustained cross-border investigations.

The last article of this conference volume 1 is Article 22, written by Kreseda Smith, who demonstrates that contemporary agricultural victimisation in Britain is increasingly experienced as organised and persistent rather than incidental, with significant implications for farmers' well-being and sector stability. Drawing on survey data from 239 farmers affected by crime in the preceding year, the analysis shows that organised agricultural criminality functions as a salient stressor – closely associated with psychological distress indicators such as anxiety, insomnia, feelings of vulnerability, loss of confidence, suicidal thoughts and considerations of exiting farming – particularly among women, younger farmers and those exposed to repeat offences. A central empirical insight concerns the disjunction between farmers' strong perception that organised crime groups are intensifying their activities in rural areas and the widespread belief that policing bodies neither recognise agricultural crime as organised nor respond effectively to reported incidents, contributing to eroded trust and perceived abandonment. Extending beyond

individual mental health effects, the article situates these experiences within broader secondary and tertiary consequences, including weakened farm viability, social withdrawal, under-reporting and longer-term risks to rural resilience and food security. On this basis, it calls for a reframing of organised agricultural crime as both a policing and public health concern, supported by improved crime classification, rural-sensitive police training, closer collaboration with farming communities and expanded comparative research capable of informing internationally relevant prevention and enforcement responses.

We hope that this volume 1 issue will be actively used as a research, training and reference resource, contributing to greater conceptual clarity and operational understanding of the complex phenomena examined across its contributions. A second volume arising from this conference will be issued immediately after this one, with more reflections around the same discussed topic: high-risk criminal networks. By bringing together empirical research, comparative analysis and practice-oriented reflection, the volume is designed not only to advance scholarly debate but also to support those engaged in professional education, policy development and operational training. I reaffirm, as the Research and Knowledge Management Officer and also Editor-in-Chief of this bulletin, a strong commitment to research-led training and to fostering dialogue between academia and practice, particularly in areas where HRCNs challenge existing institutional responses. I am confident that the insights gathered in this issue will meaningfully support the work of researchers, trainers and practitioners alike, and will serve as a durable foundation for informed analysis, effective capacity-building and future collaborative inquiry ([3]).

([3]) Generative-AI-assisted content drafted/amended.