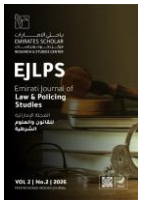

Emirati Journal of Law and Policing Studies
Vol 2 Issue 1 (2026)
Pages 40 -47
Available at
www.emiratesscholar.com

Governing Crime Without Borders: The Budapest Legacy, the Hanoi Convention, and the Future of Cross-Border Cybercrime Cooperation

Emily Carter, Valentina Ruiz
Department of Law, Harvard University, Cambridge, MA, United States, Department of Political Science, Pontifical Catholic University of Chile, Santiago, Chile

ARTICLE INFO

KEYWORDS
cybercrime; Budapest Convention; UN Convention against Cybercrime; mutual legal assistance; jurisdiction; policing cooperation; data sovereignty

HOW TO CITE
Carter, E., & Ruiz, V. (2026). Governing Crime Without Borders: The Budapest Legacy, the Hanoi Convention, and the Future of Cross-Border Cybercrime Cooperation. Emirati Journal of Law and Policing Studies, 2(1), 40-47.
https://doi.org/10.54878/2r2ssw42

ABSTRACT

Cybercrime is the paradigm case of an offence that ignores the territorial premise on which criminal law is built. A phishing operation can be authored in one country, hosted in a second, monetised through accounts in a third, and felt by victims in a hundred more, while the police who must respond remain creatures of national jurisdiction. This paper examines how the international community has tried to close that gap, from the Council of Europe' s Budapest Convention of 2001 to the United Nations Convention against Cybercrime adopted in December 2024 and opened for signature in Hanoi in October 2025. Drawing on legal analysis and the political science of regime formation, we trace the persistent trilemma at the heart of cross-border cybercrime governance: states want investigative speed, insist on sovereignty over data and process, and are pressed, unevenly, to preserve rights safeguards, and no existing instrument secures all three at once. We analyse the mutual legal assistance bottleneck, the rise of unilateral and provider-based alternatives such as the US CLOUD Act, and the negotiating cleavages that shaped the UN convention, including the human-rights objections that accompanied its adoption. A regional lens on Latin America and the Global South examines why formal accession has not translated into operational capacity, and what the new convention' s technical-assistance provisions would have to deliver to change that. We argue that the coming decade of cybercrime cooperation will be decided less by treaty text than by three quieter variables: the practical throughput of cooperation channels, the credibility of safeguards oversight, and investment in forensic and judicial capacity outside the wealthy world.

Double-blind peer review by independent reviewers.
Received: 12 Jan 2026, Accepted: 18 May2026, Published: 19 Jun 2026
*Corresponding author: emily.carter@harvard.edu

1. Introduction

Criminal law is territorial by constitution; the internet is indifferent to territory by design. Nearly every doctrinal and institutional difficulty in policing cybercrime descends from this single mismatch (Goldsmith & Wu, 2006; Brenner, 2010). When the evidence of an offence sits on a server abroad, a domestic warrant reaches the end of its authority at the border, and the investigator must either invoke slow interstate machinery, find a cooperative service provider, or act unilaterally and risk a sovereignty dispute. Each of these paths has been institutionalised somewhere in the past quarter century, and the resulting landscape is less a system than an accumulation of partial fixes.

The scale of the underlying problem is by now familiar. Cybercrime long ago industrialised: ransomware-as-a-service, phishing kits, and money-mule networks constitute a mature transnational service economy whose revenues, and whose social costs, run far ahead of enforcement capacity (Anderson et al., 2019; Europol, 2024). Attribution is hard, arrest harder, and the probability that any given offence results in a sanction is, in most of the world, close to negligible. Wall's (2007) early observation that cybercrime transforms rather than merely relocates crime remains apt: what has been transformed most is the relationship between the offence and the state expected to answer it.

The governance response reached a milestone on 24 December 2024, when the UN General Assembly adopted the United Nations Convention against Cybercrime, the first global criminal-justice treaty of the internet era; sixty-five to seventy-two states, depending on the count at close of ceremony, signed at Hanoi in October 2025 (United Nations, 2024; UNODC, 2025). Whether this instrument resolves the field's structural tensions or merely globalises them is the question of this paper. We proceed in the joint register of law and political science: doctrinal where the texts demand it, institutional where the politics do.

Section 2 reconstructs the architecture built between 2001 and 2024. Section 3 develops the sovereignty–speed–safeguards trilemma as an analytical frame and applies it to the main cooperation channels. Section 4 analyses the UN convention: what it adds, what it defers, and why its adoption divided the human-rights community. Section 5 takes up the view from the Global South, with particular attention to Latin America. Section 6 discusses implications and Section 7 concludes.

2. The Architecture of Cooperation, 2001–2025

2.1 The Budapest baseline

The Convention on Cybercrime of 2001 remains the field's foundational text (Council of Europe, 2001). Its design is threefold: harmonise substantive offences (illegal access, data and system interference, computer-related fraud and forgery, child sexual abuse material), harmonise procedural powers (expedited preservation, production orders, search and seizure of stored data, real-time collection), and build cooperation machinery (mutual legal assistance and a 24/7 point-of-contact network). Harmonisation serves cooperation: dual-criminality objections dissolve when states criminalise the same conduct, which is why a treaty formally about substantive law is functionally about extradition and evidence (Clough, 2014). Article 15 conditions the procedural powers on domestic human-rights safeguards, a clause whose significance became fully visible only when later instruments proposed weaker equivalents.

Budapest's limits are equally structural. It is a Council of Europe product with accession by invitation, and although membership grew well beyond Europe, key states, Russia, China, India, Brazil for many years, remained outside, objecting variously to its origins, to Article 32(b)'s allowance of trans-border access to data with consent, and to its perceived tilt toward Western law-enforcement interests (Clough, 2014; DeNardis, 2014). A convention cannot harmonise those who will not join it, and the world's cybercrime map came to mirror its geopolitical one.

2.2 The mutual legal assistance bottleneck

Underneath every treaty sits the working reality of mutual legal assistance, and the working reality is slow. The UNODC's global study found MLA response times for electronic evidence typically measured in months, against data that providers may retain for weeks (UNODC, 2013). The bottleneck is not malice but design: MLA routes a police request through two foreign ministries, two central authorities, and a foreign court, each applying its own thresholds, translation requirements, and queue. For volatile evidence this is a mismatch of clock speeds, and it produced predictable adaptations: informal police-to-police channels, direct requests to service providers under their voluntary-disclosure policies, and, at the limit, unilateral extraterritorial access.

The US CLOUD Act of 2018 formalised the provider channel: it asserted that US-based providers must produce

data in their possession regardless of storage location, and created executive agreements allowing qualifying foreign governments to demand data directly from US providers, bypassing MLA (Daskal, 2015, anticipated the doctrinal shift; Svantesson, 2017, its jurisdictional logic). The Second Additional Protocol to the Budapest Convention, opened for signature in 2022, moved in the same direction multilaterally, with direct cooperation provisions for subscriber information and expedited channels for emergencies. The centre of gravity has thus migrated from state-to-state assistance toward state-to-provider compulsion, a shift with large and still unsettled implications for whose law protects the data subject (Daskal, 2015; Svantesson, 2017).

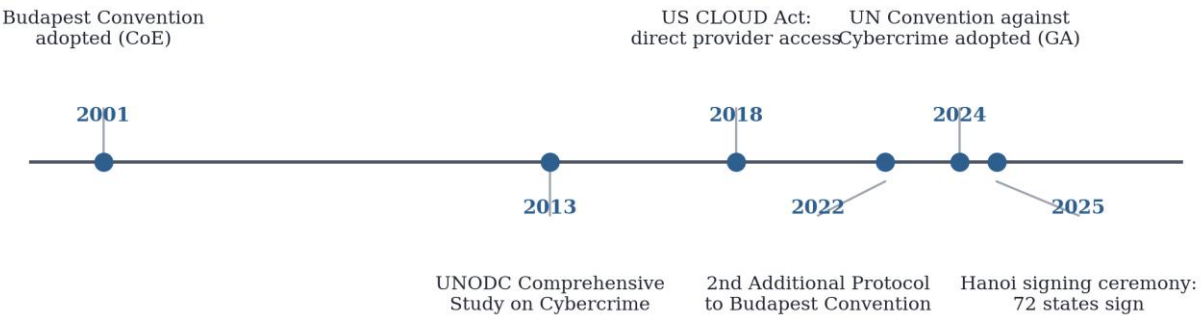

Figure 1. Milestones in cross-border cybercrime governance, 2001–2025.

2.3 The threat landscape the regime must govern

It matters for institutional design that the object of all this machinery has itself changed shape. The cybercrime economy of the mid-2000s was dominated by individually skilled offenders; today's is dominated by division of labour. Ransomware operators lease malware from developers, purchase initial access from dedicated brokers, launder proceeds through specialised mule and mixing services, and outsource negotiation with victims; phishing and investment-fraud operations run from industrial compounds whose workforce is itself often trafficked (Europol, 2024). Anderson and colleagues' cost surveys make the policy-relevant point precisely: society's losses are dominated not by the sums criminals gain but by defensive expenditure and indirect costs, and the sums spent on response dwarf the sums spent on actually pursuing offenders (Anderson et al., 2019). The implication for cooperation architecture is uncomfortable. A regime tuned to assist the investigation of individual offences confronts an adversary organised as a supply chain, whose components sit in different jurisdictions chosen partly for their non-cooperation. Disrupting a service economy requires sustained multi-jurisdictional operations against infrastructure, developers, and money flows simultaneously, exactly the kind of operation the club of capable agencies can mount (Europol, 2024) and the MLA queue cannot.

Wall's (2007) taxonomy, crimes against machines, crimes using machines, crimes in the machine, also explains why treaty scope keeps expanding. As ordinary offending migrates online, the electronic-evidence problem stops being a specialist's problem: the homicide case with a cloud-stored location history raises the same cross-border issues as the intrusion case. This is the functional logic behind the UN convention's extension of cooperation to any serious crime involving electronic evidence, and simultaneously the reason that extension alarms rights advocates, since it generalises exceptional powers to the whole of criminal procedure.

3. A Trilemma: Sovereignty, Speed, Safeguards

The recurring pattern across these instruments can be stated as a trilemma (Figure 2). Cooperation arrangements are pulled toward three goods that resist joint maximisation. Sovereignty demands that a state control criminal process and data on its territory, which implies consent-based, state-mediated channels. Speed demands that evidence move at the pace of its own volatility, which implies direct channels that cut states out. Safeguards demand independent review, notice, and proportionality, which add friction to any channel and are unevenly valued across regimes. Classical MLA maximises sovereignty and, in principle, safeguards, at ruinous cost to speed. The CLOUD Act model maximises speed at the price of the data-holding state's sovereignty and contested safeguards. Proposals that would maximise sovereignty and speed together, broad obligations to

https://doi.org/10.54878/2r2ssw42

cooperate with few grounds for refusal, are precisely those that alarm rights advocates, because the compression lands on safeguards.

The trilemma can be given a quantitative gloss. The expected sanction facing a transnational offender is the product of a chain of conditional probabilities,

P(sanction) = pdetect × pattrib × pevidence × pjurisdiction × pcustody (1)

and cross-border friction operates multiplicatively: cooperation failures at the evidence, jurisdiction, and custody links drive the product toward zero even where detection is good. This is why marginal improvements in cooperation throughput matter more than equivalent improvements in any single national capability, and why offenders rationally locate operations where the weakest links are weakest (Anderson et al., 2019; Brenner, 2010). Deterrence in cyberspace is a supply chain, and it fails at its worst node.

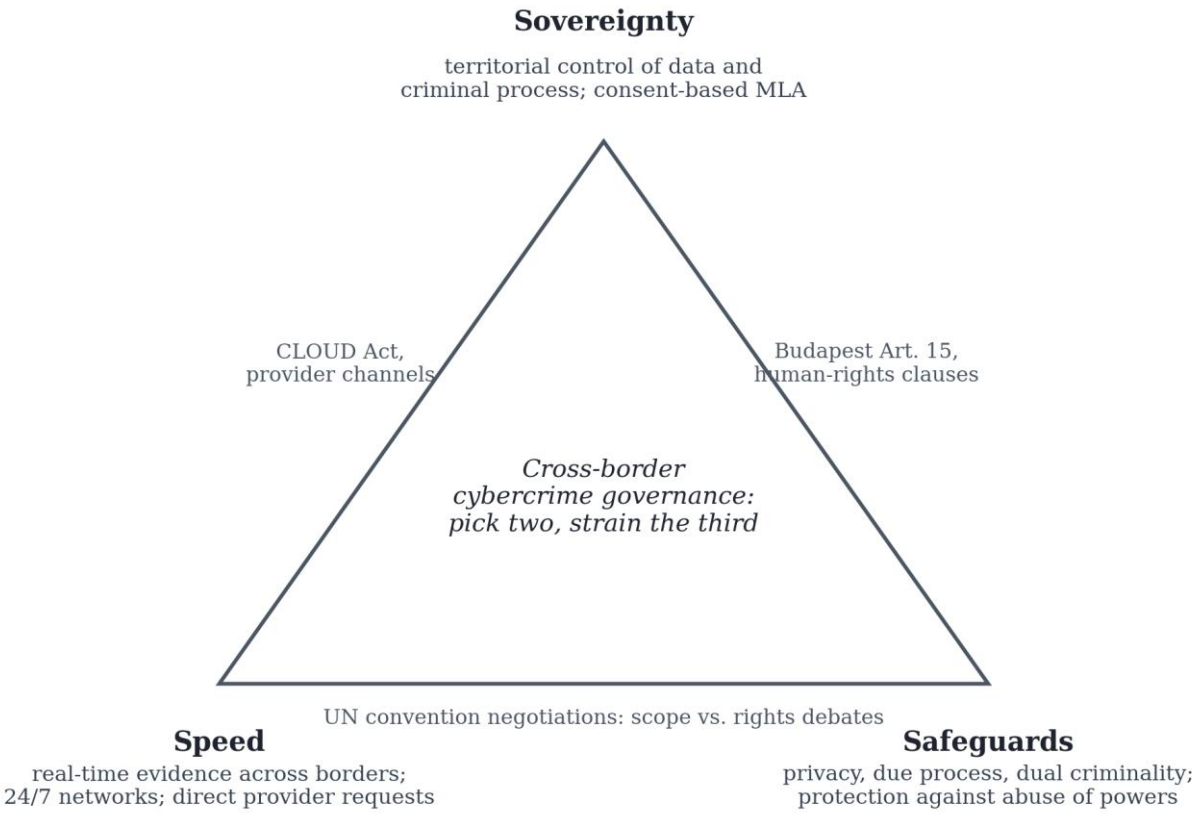

Figure 2. The sovereignty–speed–safeguards trilemma in cross-border cybercrime cooperation.

Table 1. Principal cooperation channels for cross-border electronic evidence, and their position in the trilemma.

Channel	Instrument / basis	Strength	Structural weakness
Mutual legal assistance	Bilateral MLATs; Budapest arts. 25–34; UN convention chapter on international cooperation	Sovereignty-respecting; judicially supervised	Months-long latency against weeks-long data retention (UNODC, 2013)
24/7 network points of contact	Budapest art. 35; UN convention equivalent	Rapid preservation of volatile data	Preservation is not production; follow-through still needs MLA
Direct provider requests	CLOUD Act executive agreements; Budapest 2nd Protocol; voluntary disclosure	Speed; matches where data actually sits	Bypasses data-location state; safeguards depend on provider and requesting state

Unilateral extraterritorial access	Domestic warrants asserted over foreign-stored data	No dependence on foreign consent	Sovereignty conflicts; comity disputes; precedent for authoritarian mirroring (Daskal, 2015)
Joint operations & agency channels	Europol/Interpol frameworks; joint investigation teams	Operational trust; specialisation	Club goods: effectiveness concentrated among already-capable states (Europol, 2024)

4. The UN Convention: Globalisation of the Regime, and of Its Tensions

4.1 What the convention does

The UN Convention against Cybercrime, negotiated through an Ad Hoc Committee between 2022 and 2024 and adopted by consensus on 24 December 2024, extends to all UN member states a package recognisably descended from Budapest: a core of cyber-dependent offences, procedural powers over electronic evidence, a 24/7 network, and a full chapter on international cooperation, with technical assistance and capacity building given unprecedented prominence (United Nations, 2024). Its opening for signature at Hanoi in October 2025 drew signatures from dozens of states in the treaty's first days, spanning every region and, notably, states that had refused Budapest for two decades (UNODC, 2025). As an act of inclusion, the convention succeeds where Budapest structurally could not: it is the first cybercrime instrument that Russia, China, Western states, and most of the Global South have all been able to sign.

4.2 What the controversy is about

Consensus among states was purchased at a price that civil-society observers, industry bodies, and several human-rights authorities spent the negotiation itemising. Three objections recur. The procedural powers and cooperation obligations extend beyond cyber-dependent crime to any serious offence involving electronic evidence, which converts a cybercrime treaty into a general instrument of transnational digital investigation. The safeguards clauses are thinner than Budapest's Article 15, relying heavily on domestic law in states whose domestic law is precisely the concern, with grounds for refusing cooperation narrower than rights advocates sought. And the offence definitions in some areas are broad enough to cover security research or protected expression where national implementations choose to read them so. On this view the convention resolves the trilemma by quietly de-prioritising its third vertex, and the human-rights community's near-uniform opposition at adoption is best read as a judgement about that trade (DeNardis, 2014, provides the governance frame; the critiques track debates documented throughout the negotiation record, United Nations, 2024).

A political-science reading adds a caution against both triumphalism and alarm. Treaty text is a floor for cooperation among the willing and a ceiling for very little; the operative question is which coalitions form around implementation, and whether the review mechanism the convention establishes acquires teeth. Budapest's real product was not its articles but the practice community that grew around them, the 24/7 network, the assessment rounds, the training pipelines. Whether the UN instrument grows an equivalent community, or remains a signature ceremony, is the decade's open variable (UNODC, 2025).

Table 2. The Budapest Convention (2001) and the UN Convention against Cybercrime (2024) compared.

Dimension	Budapest Convention (2001)	UN Convention (2024, 'Hanoi Convention')
Origin & membership	Council of Europe treaty; accession by invitation; ~70+ parties, key powers absent	UN treaty open to all member states; adopted by consensus; signed by 70+ states at Hanoi (2025)
Offence scope	Cyber-dependent core plus computer-related fraud, forgery, CSAM	Similar core; cooperation provisions reach any serious crime with electronic evidence
Procedural powers	Preservation, production, search/seizure, real-time collection	Equivalent suite, extended to all covered cooperation

Safeguards	Art. 15: explicit conditioning on ECHR-style protections	Safeguards clauses present but more dependent on domestic law; narrower refusal grounds
Cooperation machinery	MLA chapter; 24/7 network; 2nd Protocol adds direct-provider channels	Full cooperation chapter; 24/7 network; strong technical-assistance mandate
Review & follow-up	Cybercrime Convention Committee; assessment rounds	Conference of States Parties; mechanism design still to consolidate

4.3 Scenarios for implementation

Three futures are compatible with the text signed at Hanoi. In the convergence scenario, the UN and Budapest communities interpenetrate: overlapping membership harmonises practice, the states-parties conference adopts Budapest-style assessment rounds, and the direct-cooperation innovations of the Second Protocol diffuse into UN practice. In the parallel-regimes scenario, two practice communities consolidate around the two instruments, with cooperation flowing freely within each bloc and grudgingly between them; the trilemma is then managed not within a regime but by forum-shopping between regimes, and defendants' protections depend on which channel their data happened to travel. In the dead-letter scenario, ratification stalls below the entry-into-force threshold's practical significance, technical assistance goes unfunded, and the convention joins the family of instruments that reorganised nothing. Which scenario materialises is not written in the treaty; it will be decided by early ratifiers' practice, by whether any major data-holding state routes real cooperation through the new channels, and by the budget attached to the capacity-building chapter (United Nations, 2024; UNODC, 2025).

5. The View from the Global South

For most of the world, the binding constraint on cybercrime enforcement is not treaty membership but capacity. A convention can oblige a state to preserve data on request; it cannot conjure the forensic laboratory, the trained prosecutor, or the judge comfortable with hash values and chain-of-custody metadata for digital exhibits. The UNODC study documented the pattern a decade ago and it has not fundamentally changed: developing-country law enforcement reports shortages of specialised investigators, tools, and legal frameworks in depressing uniformity (UNODC, 2013). Forensic-science innovation continues to widen what evidence can in principle yield, from digital traces to the biological detection systems reviewed in this journal (Rawwash, 2025), but each widening also widens the gap between systems that can absorb new methods and systems that cannot.

Latin America illustrates the politics of partial integration. Much of the region acceded to Budapest over the past decade, and several states participated actively in the UN negotiations, yet operational cooperation still runs disproportionately through informal police relationships and provider goodwill, because central authorities remain understaffed and requests to Northern jurisdictions sit in the same queues as everyone else's. Regional police cooperation frameworks exist on paper; sustained funding for cyber units, less so. The result is a familiar dependency structure: evidence flows are mediated by the handful of jurisdictions, and the handful of companies, where the world's data resides, and Southern agency in the regime consists largely of choosing which Northern channel to petition (DeNardis, 2014; Svantesson, 2017).

Institutional accountability is the underappreciated variable here. Cooperation channels transmit trust as much as data: a requested state's willingness to serve a warrant, and a provider's willingness to disclose, depend on confidence in the requesting state's courts. Work on international standards of judicial accountability, including in this journal (Ismaili, 2025), bears directly on cybercrime cooperation for that reason: independent, accountable judiciaries are not an ornament of the regime but part of its transmission mechanism, since safeguards-based refusal grounds are operated by exactly these institutions. States seeking faster inbound cooperation have, in the judicial-integrity agenda, a lever that requires no treaty at all. The same logic extends to the technological modernisation of policing itself: the smart-city and AI-enabled enforcement platforms now being piloted in the Gulf and elsewhere (Sabeh, 2025) will generate precisely the categories of data, and the categories of dispute, that the new convention's powers govern, and they will do so first in jurisdictions whose oversight institutions are still consolidating.

The pattern generalises beyond Latin America with regional inflections. In Africa, the Malabo Convention's slow ratification history foreshadowed the gap between signature and operation that now confronts the UN instrument, and national cybercrime statutes adopted in its wake have repeatedly doubled as instruments against

journalists and opposition figures, illustrating concretely why safeguards floors matter most where oversight institutions are youngest. In South and Southeast Asia, dense digital economies coexist with cooperation frameworks fragmented among bilateral arrangements, and the region's emergence as both a major victim pool and a major hosting environment for industrial-scale fraud compounds gives it the strongest material interest in a functioning global regime (Europol, 2024; UNODC, 2013). Across all three regions the deeper point is the same: the distribution of cybercrime's costs and the distribution of investigative capability have come apart, and the new convention's legitimacy in the South will be judged by whether it narrows that gap or merely codifies it.

Table 3. Capacity and integration constraints on cybercrime cooperation in developing regions, with corresponding provisions of the 2024 UN convention.

Constraint	Manifestation	Relevant UN convention response	Residual gap
Forensic capacity	Few accredited digital-forensics labs; backlogged devices	Technical assistance and capacity-building chapter	Funding is voluntary; no entitlement
Central-authority throughput	Small MLA units; multi-month latency both directions	24/7 network; streamlined cooperation forms	Staffing is domestic; treaty cannot supply it
Judicial familiarity	Digital evidence contested or over-admitted; weak precedent	Training mandates; states-parties conference exchange	Depends on judicial-accountability reform (Ismaili, 2025)
Provider leverage	No domestic providers; dependence on foreign voluntary disclosure	Cooperation obligations among parties	Major providers' home states set effective policy
Rights oversight	Data-protection and oversight bodies young or absent	Safeguards clauses referencing domestic law	Thin floor where domestic law is thin

6. Discussion

6.1 Three variables that will decide the decade

The first is throughput. Whatever instruments say, cooperation is experienced by investigators as a latency distribution, and by defendants as the set of protections that survived the shortcut taken. Measuring MLA and direct-request turnaround publicly, per country pair, would do more to discipline the system than a further round of norm-making; what is measured queues differently. The second is safeguards credibility. The direct-provider channels that now carry increasing volume rest on certifications that requesting states meet rights baselines. If those certifications come to be seen as diplomatic fictions, the channels will face domestic-court resistance in data-holding states, and speed will collapse back into litigation. Safeguards, in other words, are not a tax on cooperation but a condition of its durability. The third is capacity investment. The UN convention's most consequential chapter may prove to be its least glamorous: technical assistance. A regime whose Southern members can preserve, but never independently produce or analyse, evidence will reproduce the dependency structure that made a UN instrument politically necessary in the first place.

6.2 What research should watch

The empirical agenda that follows from this analysis is concrete. Cooperation latency should be studied as an outcome variable: request-to-response distributions across channel types and country pairs would let scholars test, rather than assert, whether treaty membership changes practice. The certification politics of direct-provider channels deserve case-study attention, since they are where safeguards claims meet institutional facts. Ratification and reservation behaviour on the UN convention offers political scientists a natural experiment in regime design, with the human-rights controversy providing clearly articulated rival predictions. And the interaction between new enforcement technologies and cooperation demand, as AI-enabled policing platforms of the kind now deployed in smart-city contexts generate cross-border evidence of their own (Sabeh, 2025), remains almost entirely unstudied. Each of these is tractable with public data and patience; none requires access to classified operations.

6.3 Limitations

Two limitations bound this analysis. The UN convention is newly signed and unratified as we write; its entry into force, reservations practice, and review-mechanism design will resolve questions we can only frame, and our characterisation of negotiating positions relies on the public record of a process whose decisive bargaining was informal. And our regional analysis foregrounds Latin America as an illustrative case of the Global South's position; Africa, South and Southeast Asia present distinct configurations, particularly where regional instruments overlap, that deserve dedicated treatment.

7. Conclusion

Twenty-five years separate Budapest from Hanoi, and the distance is instructive. The field began with a club of like-minded states harmonising law in the expectation that cooperation would follow, and arrived at a universal treaty whose universality was achieved by loosening the very safeguards that made the club trustworthy to its members. That is not hypocrisy; it is the trilemma doing its work at global scale. The practical agenda that follows is unheroic: publish cooperation metrics, resource central authorities, make safeguards certifications honest enough to survive judicial scrutiny, fund forensic and judicial capacity where it is absent, and let the new convention's implementation community, not its text, determine what it becomes. Cybercrime governance will not be solved; it will be administered, well or badly. The difference between those two futures is decided in budget lines and oversight hearings, which is to say, in the ordinary machinery of law and politics that cyberspace was once imagined to have escaped.

Declarations

Conflict of interest. The authors declare no conflict of interest.

Funding. This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Acknowledgements. The authors thank colleagues at their respective departments for comments on an earlier draft.

References

Anderson, R., Barton, C., Böhme, R., Clayton, R., Gañán, C., Grasso, T., Levi, M., Moore, T., & Vasek, M. (2019). Measuring the changing cost of cybercrime. Workshop on the Economics of Information Security (WEIS 2019).

Brenner, S. W. (2010). Cybercrime: Criminal threats from cyberspace. Praeger.

Clough, J. (2014). A world of difference: The Budapest Convention on Cybercrime and the challenges of harmonisation. Monash University Law Review, 40(3), 698–736.

Council of Europe. (2001). Convention on Cybercrime (ETS No. 185). Council of Europe.

Daskal, J. (2015). The un-territoriality of data. Yale Law Journal, 125(2), 326–398.

DeNardis, L. (2014). The global war for internet governance. Yale University Press.

Europol. (2024). Internet Organised Crime Threat Assessment (IOCTA) 2024. Publications Office of the European Union.

Goldsmith, J., & Wu, T. (2006). Who controls the Internet? Illusions of a borderless world. Oxford University Press.

Ismaili, H. (2025). International standards for judicial accountability and the accountability of the judiciary. Emirati Journal of Law and Policing Studies, 1(1). Emirates Scholar Center for Research and Studies.

Rawwash, A. A. (2025). The role of honeybees in forensic evidence detection: Review of their application in environmental and criminal investigations. Emirati Journal of Law and Policing Studies, 1(1), 4–16. Emirates Scholar Center for Research and Studies. https://doi.org/10.54878/wafkw950

Sabeh, R. M. (2025). Traffic congestion in Sharjah: Strategies between urban growth and innovation. Emirati Journal of Law and Policing Studies, 1(1), 48–59. Emirates Scholar Center for Research and Studies. https://doi.org/10.54878/53c4m385

Svantesson, D. J. B. (2017). Solving the internet jurisdiction puzzle. Oxford University Press.

United Nations. (2024). United Nations Convention against Cybercrime (A/RES/79/243, adopted 24 December 2024). United Nations.

United Nations Office on Drugs and Crime. (2013). Comprehensive study on cybercrime. UNODC.

United Nations Office on Drugs and Crime. (2025, October). UN Convention against Cybercrime opens for signature in Hanoi, Viet Nam [Press release]. UNODC.

Wall, D. S. (2007). Cybercrime: The transformation of crime in the information age. Polity Press.