Traditional mutual legal assistance mechanisms often prove woefully inadequate in addressing such transnational complexity

Law beyond borders: the UN Cybercrime Convention navigating legal challenges in cross-border digital threats

by **Prof. Dr. Vladimir Aras**

In December 2024, through resolution 79/243, the United Nations General Assembly unanimously adopted the UN Convention against Cybercrime, marking a watershed moment in international criminal law.[1] This landmark treaty, the first comprehensive global cybercrime framework in over two decades, represents both humanity's collective recognition of digital threats and our evolving capacity to address them through multilateral cooperation.

The borderless challenge

Cybercrime has fundamentally transformed the criminal landscape, creating a paradox where the most sophisticated crimes occur in a realm that knows no borders, yet must be prosecuted within systems built on territorial sovereignty. Today's cybercriminals and threat actors operate with unprecedented impunity, exploiting jurisdictional gaps, regulatory inconsistencies, and the growing speed differential between technological innovation and legal adaptation.

Consider the anatomy of a modern ransomware attack: perpetrators in one jurisdiction infiltrate systems in another, encrypt data stored across multiple countries, demand payment through cryptocurrency networks spanning the globe, and launder proceeds through digital exchanges in yet other territories.[2] Traditional mutual legal assistance mechanisms often prove woefully inadequate in addressing such transnational complexity.

The challenge extends beyond mere logistics. Digital evidence is inherently volatile – easily altered, deleted, or relocated across servers worldwide within minutes.[3] The asymmetry between

[1] United Nations General Assembly, "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", December 2024.

[2] Chainalysis Team, "OFAC Sanctions Fraud Network Funding DPRK Weapons Programs", August 2025.

[3] Aurang Zaib Ashraf Shami, "Cybercrime and Digital Evidence: investigating the challenges and opportunities in prosecuting cybercrime and handling digital evidence", Research Consortium Archive, August 2025.

the speed of cybercrime and the pace of international legal cooperation creates a systematic advantage for criminals, who can outmanoeuvre law enforcement constrained by bureaucratic processes and sovereignty concerns.

A global response takes shape

The UN Cybercrime Convention emerges against this backdrop as an ambitious attempt to harmonize international responses to digital threats. Building upon the normative foundations laid by the 2001 Budapest Convention, the UN treaty attains an unparalleled degree of international legitimacy, evidenced by its unanimous endorsement by all 193 Member States.[4]

The Convention's architecture reflects hard-won compromises between competing visions of cybersecurity governance. It establishes standardized definitions for core offenses – illegal access, cyber fraud, online child exploitation – while creating mechanisms for rapid international cooperation through a 24/7 network system. States parties must criminalize illegal access to ICT systems; illegal interception of non-public transmissions of electronic data; interference with electronic data or ICT systems; misuse of devices that facilitate the commission of such offences; ICT system-related forgery; ICT system-related theft or fraud; offences related to online child sexual abuse or child sexual exploitation material; solicitation or grooming for the purpose of committing a sexual offence against a child; non-consensual dissemination of intimate images; and laundering of proceeds of the above offences. Most significantly, it emphasizes prevention strategies, technical assistance and capacity building, recognizing that cybersecurity is only as strong as its weakest link.

The treaty's provisions on international cooperation represent its most innovative elements. Traditional extradition processes, which can take years, are supplemented by streamlined evidence-sharing mechanisms designed to preserve digital evidence before it disappears. The Convention mandates that States designate competent authorities available 24/7 to respond to urgent requests for assistance, acknowledging that cybercrime operates on Internet time, not bureaucratic schedules. In addition, the Convention establishes a comprehensive multilateral framework designed to facilitate cooperation in transnational criminal matters, encompassing investigative activities, prosecutorial coordination, mechanisms for asset recovery, and the conduct of judicial proceedings.[5]

Opportunities and tensions

> **“The significance of the Convention resides not solely in the normative duties it codifies, but also in its capacity to cultivate a transnational community of practice in the prevention and prosecution of cybercrime.”**

By operationalizing States’ positive obligations under international law, the instrument reinforces the principle of due diligence in cyberspace, obliging States to adopt effective measures to prevent, investigate, and punish transnational offences facilitated by digital technologies.[6] In this sense,

[4] Hanoi Convention, “Official Statement”.

[5] Do Viet Cuong and Nguyen Quang Ha, “Hanoi Convention against Cybercrime: a milestone for the World and Vietnam”, Vietnam Law Magazine, April 2025.

[6] Carmen Eloísa Ruiz López, Vladimir Barros Aras, “A ação penal como um remédio efetivo para a defesa de direitos humanos: uma visão a partir da jurisprudência das cortes regionais”, Revista jurídica da presidência, March 2024.

the Convention not only harmonizes substantive and procedural norms but also institutionalizes mechanisms of mutual legal assistance and cross-border cooperation, particularly in the areas of evidence preservation, information-sharing, and judicial cooperation. The result is a normative framework that strengthens both horizontal collaboration among States and vertical accountability to international legal standards, thereby contributing to the consolidation of an integrated regime of global cyber governance. By establishing common standards and facilitating knowledge transfer from technologically advanced nations to developing countries, it promises to level the playing field against transnational criminal networks.

Yet the treaty's ambitions are tempered by significant concerns. Critics, including several civil society organizations, warn that vague language could criminalize legitimate security research and expand state surveillance powers without adequate safeguards.[7] The Convention's broad definitions–particularly those relating to "electronic data" and "information and communications technology system" – could create a framework susceptible to authoritarian abuse. I do not consider this to be accurate, given that the Convention is grounded in universally recognised human rights principles.

But some human rights issues are particularly troubling. While the treaty references international human rights law, it largely defers substantive protections to national legislation. This creates a dangerous precedent where authoritarian regimes could potentially use the Convention's cooperation mechanisms to pursue dissidents, whistleblowers, or journalists under the guise of cybercrime enforcement.

The path forward

The Convention's true test will come not in its formal ratification – expected to occur rapidly given its unanimous adoption – but in its implementation across diverse legal systems and political contexts. Following an extended negotiation process, the Convention was made available for signature on 25 October 2025 during a ceremony in Hanoi, Viet

[7] Kate Graham-Shaw, "New U.N. Cybercrime Treaty Could Threaten Human Rights", Scientific American, August 2024.

Nam, and will remain open for signature at United Nations Headquarters in New York until 31 December 2026. It is set to enter into force upon the deposit of the fortieth instrument of ratification or accession, after which its implementation will be subject to review by the Conference of the States Parties.

Success will require a careful balance between security imperatives and rights protections, international cooperation and sovereignty concerns, technological innovation and legal certainty. The Convention must evolve beyond a mere legal instrument to become a framework for ongoing dialogue and adaptation as digital threats continue to evolve. The stakes could not be higher. As digital technologies become increasingly central to economic activity, social interaction, and democratic governance, the failure to establish effective international cooperation against cybercrime threatens not only individual security but the integrity of the digital commons upon which modern society depends. We trust that the Convention will not only enter into force without delay, but will also secure wide ratification, thereby consolidating its authority as a universal instrument of international law.

Conclusion

The UN Cybercrime Convention represents both an achievement and a beginning. It demonstrates unprecedented global consensus on the need for coordinated responses to digital threats while highlighting the persistent tensions between security and freedom in the digital age. Its ultimate success will depend not on the elegance of its legal architecture but on the wisdom and restraint with which it is implemented by the international community, especially by prosecutors and courts across the globe.

As we stand at this inflection point, the Convention offers a framework for international cooperation that, if properly implemented with robust human rights safeguards, could significantly enhance global cybersecurity.

The choice before us is clear: we can use this moment to build a more secure and rights-respecting digital future, or we can allow legitimate security concerns to justify the erosion of the freedoms that make the digital revolution worthwhile.

> **“The UN Cybercrime Convention provides the framework; the global community must provide the wisdom to use it well.”**

About the Author

Vladimir Aras holds a PhD in Law, a Master's degree in Public Law, an MBA in Public Management, and has been a member of the Public Prosecutor's Office since 1993. He is a Senior Federal Prosecutor in Brasília, Adjunct Professor of Criminal Procedure and International Law (UnB), a member of the Attorney General's Office's (PGR) Cybercrime Task Force (GACCTI), former Head of the International Cooperation Unity within the PGR (2013-2017), and Founder of the Institute of Law and Innovation (ID-i).

unicri

University for Peace

MASTER OF LAWS (LL.M.)

in Global Criminal Justice and Accountability

16 November 2026 - 25 June 2027, Turin (Italy)

Apply by 6 September 2026

Scan for more

Explore our Master of Laws (LL.M.) program at www.unicri.org and take the next step in your legal education

unicri

University for Peace

MASTER OF LAWS LLM

IN CYBERCRIME, CYBERSECURITY AND INTERNATIONAL LAW