



JOANNA KULESZA

University of Lodz

ORCID: 0000-0003-0390-6062

joanna_kulesza@wpia.uni.lodz.pl

Two Frameworks, One Threat: Securitisation, Corporate Power, and the Future of International Cybersecurity Governance

Dwa reżimy, jedno zagrożenie.

Sekurytyzacja, siła korporacji i przyszłość międzynarodowego zarządzania cyberbezpieczeństwem

Keywords:

cybersecurity,
UN Global Mechanism,
Hanoi Convention,
securitisation, technology
companies, international
law, OSCE

Słowa kluczowe:

cyberbezpieczeństwo,
Mechanizm Globalny
ONZ, Konwencja z Hanoi,
sekurytyzacja, firmy
technologiczne, prawo
międzynarodowe, OBWE



Two Frameworks, One Threat: Securitisation, Corporate Power, and the Future of International Cybersecurity Governance

March 2026 marked a historic moment for international cybersecurity: the first meeting of the United Nations Permanent Mechanism on cybersecurity took place only a few months after the formal signing of the UN Convention on Cybercrime (the Hanoi Convention). Both instruments seek to regulate complementary areas of international relations, yet they rest on fundamentally different regulatory logics. Drawing on the Copenhagen School securitisation theory, this article argues that cyberspace is the object of two competing securitising moves – one framing it as a domain of international peace and security, the other as a transnational criminal threat – and that the resulting governance architecture is co-produced not only by states but also by transnational technology corporations whose infrastructural and normative authority supplies the technical content that makes such threat constructions credible. The article analyses the institutional architecture of the UN Permanent Mechanism, the December 2025 ICC Prosecutor's policy on cyber-enabled crimes, and the role of private technology actors in shaping international legal norms.

Dwa reżimy, jedno zagrożenie. Sekurytyzacja, siła korporacji i przyszłość międzynarodowego zarządzania cyberbezpieczeństwem

Marzec 2026 r. to historyczny moment dla międzynarodowego cyberbezpieczeństwa: pierwsze posiedzenie Stałego Mechanizmu ONZ ds. cyberbezpieczeństwa zbiega się w czasie z otwarciem do ratyfikacji konwencji ONZ o cyberprzestępczości (konwencji z Hanoi). Oba instrumenty zmierzają do uregulowania komplementarnych obszarów stosunków międzynarodowych, opierając się jednak na zasadniczo odmiennych założeniach regulacyjnych. W oparciu o teorię sekurytyzacji szkoły kopenhaskiej artykuł stawia tezę, że cyberprzestrzeń jest przedmiotem dwóch konkurencyjnych zabiegów sekurytyzacyjnych – jako płaszczyzna pokoju i bezpieczeństwa międzynarodowego oraz jako przestrzeń ponadnarodowego zagrożenia działalnością przestępczą – a wynikająca z nich architektura zarządzania jest współtworzona nie tylko przez państwa, lecz także przez globalne korporacje technologiczne, za sprawą władzy sprawowanej przez nie nad infrastrukturą, która leży u źródeł zagrożenia. Artykuł analizuje architekturę Stałego Mechanizmu ONZ, politykę prokuratora MTK z grudnia 2025 r. w sprawie przestępstw popełnianych z wykorzystaniem technologii cyfrowych (*cyber-enabled crimes*) oraz rolę prywatnych podmiotów technologicznych w kształtowaniu norm prawa międzynarodowego. Jako punkt odniesienia dla formułowanych rekomendacji wykorzystano doświadczenia OBWE w obszarze polityki dotyczącej środków budowania zaufania w cyberprzestrzeni.

Introduction

On 30 March 2026, all 193 UN member states convened in New York to launch the Global Mechanism on Developments in the Field of Information Computer Technologies (ICTs) in the Context of International Security and Advancing Responsible State Behaviour in the Use of ICTs, the United Nations' first permanent institutional forum for cybersecurity.¹ The establishment of the Global Mechanism concludes more than two decades of fragmented multilateral effort, from the first Group of Governmental Experts (GGE) in 2004 through six successive GGEs and two Open-Ended Working Groups (OEWGs). It constitutes a genuine political achievement in a domain characterised by deep ideological disagreement between democratic and authoritarian blocs.²

Almost simultaneously, the UN Convention against Cybercrime, negotiated under the auspices of the General Assembly's Third Committee and adopted in Hanoi, entered the ratification process. While the Global Mechanism is the product of the First Committee's tradition of arms control and international security deliberation, the Hanoi Convention addresses cybercrime as a matter of criminal law and law enforcement cooperation. It requires states to criminalise a defined catalogue of offences and to cooperate in their investigation and prosecution.³

The coexistence of these two frameworks might appear complementary. One governs state behaviour in cyberspace as a matter of international security; the other harmonises national criminal law and its enforcement. In practice, however, the boundary between them is neither clean nor stable. Cyberspace does not respect institutional divisions. The same

- 1 United Nations General Assembly, *Developments in the Field of Information and Telecommunications in the Context of International Security. Note by the Secretary-General Transmitting the Final Report of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025*, 2025.
- 2 United Nations General Assembly, Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025, *Final Report of the Open-Ended Working Group*, 2025.
- 3 United Nations General Assembly, *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*, 2024.

attack on a hospital's information systems may simultaneously trigger three distinct legal regimes.⁴ If it occurs in an armed conflict, it may constitute a war crime under the framework set out in the ICC's new cyber policy.⁵ It may also constitute a cybercrime under national law, of the kind the Hanoi Convention addresses, and to a violation of the voluntary norms for responsible state behaviour that the Global Mechanism is designed to promote. The governance architecture being constructed in 2026 assigns these overlapping phenomena to different fora, different legal regimes, and different communities of practice, with very limited structural connections between them. From the perspective of securitisation theory, the same set of facts is therefore the object of competing securitising claims, advanced through different institutional channels by different speakers.

This fragmentation matters because the actors shaping cyberspace are not similarly compartmentalised. Technology companies – providers of cloud infrastructure, operating systems, communication platforms, and the specialised tools of offensive and defensive cyber operations – inhabit all these domains simultaneously. Their design choices, their terms of service, their decisions about where to store data and under what conditions to share it with governments, and their lobbying in multilateral fora all shape what is technically possible for states, criminals, and international institutions alike.⁶

The central argument of this article is that the parallel-track architecture of 2026 systematically underestimates the degree to which private technological actors have become co-authors of international norms, and

4 This example is illustrative; analogous reasoning is developed in: International Criminal Court, *Policy on Cyber-Enabled Crimes under the Rome Statute*, 2025.

5 Ibidem.

6 On the fragmentation of global governance and the growing role of non-state and transnational actors in shaping security domains, see: James N. Rosenau, *Along the Domestic-Foreign Frontier: Exploring Governance in a Turbulent World* (Cambridge: Cambridge University Press, 1997); Anne-Marie Slaughter, *A New World Order* (Princeton: Princeton University Press, 2004); Thomas Risse, ed., *Governance without a State? Policies and Politics in Areas of Limited Statehood* (New York: Columbia University Press, 2011); Martha Finnemore, and Duncan B. Hollis, "Constructing Norms for Global Cybersecurity," *American Journal of International Law* 110 (2016): 425–479; Joseph S. Nye Jr., *The Regime Complex for Managing Global Cyber Activities* (Waterloo and London: Centre for International Governance Innovation and Chatham House, 2014).

that this underestimation will limit the effectiveness of both the Global Mechanism and the Hanoi Convention.

Theoretical framework, hypothesis and method

This article adopts the securitisation framework developed by the Copenhagen School. In the formulation of Barry Buzan, Ole Waever and Jaap de Wilde, securitisation is a discursive process in which a securitising actor frames an issue as an existential threat to a referent object, thereby seeking to legitimise extraordinary measures that would not be acceptable in ordinary politics.⁷ The framework distinguishes three roles: the securitising actor (typically a state or political elite), the referent object (that which is to be protected), and functional actors – entities that significantly affect decisions in the field of security without themselves being the securitising actor or the referent object.⁸ This study argues that the cyber domain blurs the boundary between securitising actors and functional actors because the technical authority required to define the threat is increasingly held by transnational technology corporations rather than states.

The article advances a single central hypothesis: the parallel emergence of the UN Global Mechanism and the Hanoi Convention reflects two distinct securitising moves – one framing cyberspace as a domain of international peace and security, the other framing it as a transnational criminal threat – and the resulting governance architecture is shaped not only by states as traditional securitising actors but also by transnational technology corporations whose infrastructural and normative authority co-produces the threat construction. Three subsidiary research questions structure the analysis. First, how do the Global Mechanism and the Hanoi Convention differ in their underlying regulatory logic, and what governance gaps does that difference produce? Second, what role do transnational technology corporations play in shaping both frameworks, and how does that role complicate state-centric accounts of international norm formation? Third, what lessons can be drawn from the OSCE experience for

7 Barry Buzan, Ole Waever, and Jaap de Wilde, *Security: A New Framework for Analysis* (Boulder: Lynne Rienner, 1998): 23–26.

8 Ibidem: 35–42.

closing the resulting governance gaps without abandoning the intergovernmental character of either framework?

The article adopts a qualitative, analytical-interpretive approach.⁹ It draws on three categories of primary sources: UN documents (OEWG and GGE reports, the Hanoi Convention text, the December 2025 ICC OTP policy), regional instruments (OSCE PC.DEC/1106 and PC.DEC/1202), and statements of major technology corporations and civil society organisations participating in these processes. These are read against the secondary literature on securitisation theory and cyber norm formation. Cases are selected for their political and institutional centrality rather than statistical representativeness. The OSCE confidence-building framework is used as a comparative reference point throughout, particularly in section six, because it is the most institutionally developed regional analogue to the global mechanism and offers operational lessons beyond those that can be derived from a purely conceptual analysis of the UN process. The article proceeds as follows. Section two examines the architecture of the Global Mechanism. Section three analyses the Hanoi Convention as a parallel track. Section four maps the governance gap between them and the ICC's bridging attempt. Section five develops the argument about technology companies as norm co-authors. Section six draws on OSCE experience to formulate recommendations. Section seven concludes.

The Global Mechanism – architecture and ambition

From ad hoc groups to a permanent forum

The establishment of a permanent UN forum for cybersecurity discussions is a story about institutional persistence overcoming geopolitical resistance. Since 1998, when the Russian Federation introduced the first UN General Assembly resolution on developments in the field of information and telecommunications in the context of international security, the question of how to govern state behaviour in cyberspace has been on the UN agenda.¹⁰

9 On the methodology of qualitative document analysis in international relations research, see Audie Klotz, Deepa Prakash, eds., *Qualitative Methods in International Relations: A Pluralist Guide* (Basingstoke: Palgrave Macmillan, 2008).

10 United Nations, *Developments in the Field of Information and Telecommunications in the Context of International Security*, 1998.

Progress was slow, punctuated, and frequently hostage to broader great-power competition.¹¹

The key substantive achievements of this process, collected under the rubric of the framework for responsible state behaviour, are nonetheless significant. In 2013 states affirmed that international law, including the UN Charter, applies in cyberspace. They agreed on 11 voluntary, non-binding norms for responsible state behaviour in 2015. They adopted principles on cyber capacity-building in 2021. They developed universal confidence-building measures, including a global Points of Contact directory (2022–2024). The final report of the Open-Ended Working Group explicitly presents these elements as mutually reinforcing components of a single framework, combining the applicability of international law, voluntary norms, confidence-building measures, and capacity-building as the central pillars of international cybersecurity governance.

The debate over institutional form was itself politically charged. Russia's preference for a permanent OEWG with exclusive plenary sessions reflected a desire to maintain a broad, state-centric forum resistant to an implementation agenda.¹² France's Programme of Action proposal, backed by the EU, envisaged a combination of plenary meetings and working groups focused on translating agreed norms into practice.¹³ The compromise reached in July 2025 – a permanent Global Mechanism with formal plenary sessions and informal Dedicated Thematic Groups (DTGs) – reflects elements of all three competing approaches and satisfies none of them entirely.

The DTGs – promise and uncertainty

The DTGs are the mechanism's most consequential institutional innovation. Two DTGs have been established for the first four-year cycle. DTG 1 focuses on addressing specific challenges in the sphere of ICT security

11 See e.g.: Tim Maurer, *Cyber Norms: Why International Cooperation on Cybersecurity Is Failing* (New York: Council on Foreign Relations, 2011); James A. Lewis, *Creating Accountability for Global Cyber Norms* (Washington: Center for Strategic and International Studies, 2022), accessed 16 June 2026, <https://www.csis.org/analysis/creating-accountability-global-cyber-norms>.

12 United Nations, *Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025*, 2020.

13 Republic of France, *Programme of Action (PoA) to Advance Responsible State Behaviour in the Use of ICTs in the Context of International Security*, 2023.

in the context of international security. DTG 2 focuses on accelerating ICT security capacity-building. Both will operate in hybrid format as informal meetings, with formal decision-making remaining with the plenary. The informality of the DTGs is both their strength and their limitation.¹⁴

The final report of the Open-Ended Working Group explicitly presents the future permanent mechanism as a forum intended not only to preserve the past consensus but to support the practical implementation of previously agreed norms, confidence-building measures, and capacity-building commitments.¹⁵ Yet several critical design questions remain unresolved as of the mechanism's launch: the specific agenda items and thematic focus of each DTG; the nature and status of their recommendations to the plenary; and the modalities for engaging non-governmental experts. The annex to the report sets out the general structure of the mechanism but leaves significant room for interpretation as to how these elements will function in practice.¹⁶

The framework and its gaps

The framework for responsible state behaviour that the Global Mechanism inherits is a political achievement and an analytically incomplete project simultaneously. It affirms that international law applies in cyberspace without resolving most of the hard questions about how it applies. It establishes voluntary norms without creating mechanisms for their verification or enforcement. It develops confidence-building measures without addressing the attribution problem that makes them difficult to operationalise in practice. The final report of the Open-Ended Working Group reaffirms the continued applicability of core principles of international law, including sovereignty, non-intervention, and the prohibition of the use of force, thereby confirming that the emerging cybersecurity framework remains firmly rooted in traditional legal concepts.¹⁷

14 Christina Rupp, *The UN's New Global Mechanism on Cybersecurity: How Europe Can Advance Responsible State Behaviour in Cyberspace* (Berlin: Interface, 2026).

15 United Nations General Assembly, *Final Report of the Open-ended*, 2025.

16 Rupp, *The UN's*.

17 United Nations General Assembly, *Developments*, 2025; United Nations General Assembly, *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, 2021.

Most significantly, the framework was constructed through a process that was formally intergovernmental but substantively shaped by actors other than governments, including private companies, civil society organisations, and independent academic experts.¹⁸ The Tallinn Manual process, which has produced the most authoritative academic analysis of how international law applies to cyber operations, was facilitated by NATO's Cooperative Cyber Defence Centre of Excellence and carried out by groups of independent experts.¹⁹ The ICC's new cyber policy explicitly acknowledges the Tallinn Manual as an aid to interpretation.²⁰ This illustrates how private actors have effectively contributed to international legal interpretation without any formal mandate from states.

This phenomenon can be more precisely explained through the lens of contemporary international relations theory. The increasing role of non-state actors in the interpretation and operationalisation of international law reflects a shift away from a purely state-centric model of norm formation towards a more complex structure in which technological capacity itself becomes a source of political influence.²¹ In the context of cyberspace, the ability to design and control digital infrastructure may generate forms of power that function alongside, and sometimes independently from, traditional military or economic capabilities.²² The development of cybersecurity norms should therefore be analysed not only as a legal process but also as a transformation in the structure of international power relations.

18 Martha Finnemore, and Duncan B. Hollis, "Constructing Norms for Global Cybersecurity," *American Journal of International Law* 110 (2016): 425–479; Allison Pytlak et al., *The Rules of the Road in Cyberspace, 10 Years Later* (London: Royal United Services Institute, 2025).

19 Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017).

20 International Criminal Court, *Policy*.

21 Joanna Kulesza, and Jacqueline Eggenschwiler, "Non-State Actors as Shapers of Customary Standards of Responsible Behavior in Cyberspace," in *Governing Cyberspace: Behavior, Power and Diplomacy*, ed. Dennis Broeders, and Bibi van den Berg (London: Rowman and Littlefield International, 2020): 245–262.

22 Lucas Kello, *The Virtual Weapon and International Order* (New Haven: Yale University Press, 2017).

The Hanoi Convention – a parallel track

Origins and scope

The UN Convention against Cybercrime – the Hanoi Convention – represents the culmination of a separate, though contemporaneous, multilateral process. Negotiated under an Ad hoc Committee established in 2019, it aims to harmonise national laws criminalising cyber-dependent and cyber-enabled offences and to establish frameworks for international law enforcement cooperation. It follows, and in some respects expands upon, the 2001 Council of Europe's Budapest Convention on Cybercrime and its Additional Protocols.²³

The subject matter of the Hanoi Convention is, in principle, distinct from that of the Global Mechanism. Where the Global Mechanism addresses state behaviour in cyberspace as a matter of international security, the Hanoi Convention addresses cybercrime: offences committed by individuals or groups, punishable under national law. The ICC's December 2025 cyber policy makes the distinction explicit. The Court does not have jurisdiction over ordinary cybercrimes that are punishable under domestic law, even though such conduct may also amount or otherwise be relevant to crimes within the Court's jurisdiction.

The divergence in design logic

The Hanoi Convention and the Global Mechanism embody fundamentally different design logics. The Global Mechanism operates on the logic of political norms and voluntary frameworks. Its outputs constitute soft law: they express shared expectations and provide frameworks for coordination without creating binding obligations. The Hanoi Convention, by contrast, operates on the logic of binding treaty law and mutual legal assistance. Once it enters into force, it will require parties to criminalise defined offences, establish jurisdiction over them, and cooperate with other parties in their investigation and prosecution.

These different logics might be complementary if the phenomena they address were cleanly separable. But they are not. A state-sponsored hack-

23 United Nations, *Convention against Cybercrime*, 2024; Council of Europe, *Convention on Cybercrime*, 2001.

ing group that accesses another state's critical infrastructure is simultaneously violating the voluntary norms affirmed under the OEWG framework, potentially committing an act that could be characterised as aggression or a war crime if it occurs in armed conflict and causes sufficient harm, and engaging in conduct that constitutes illegal access to a computer system under the Hanoi Convention. Yet for the latter category, the Convention provides no mechanism to address such conduct when perpetrated by state actors. This reveals the most significant structural gap between the two frameworks. The Hanoi Convention is designed for non-state actors; the Global Mechanism addresses state behaviour through voluntary norms with no enforcement mechanism. Read through the lens of securitisation theory, this gap reflects the fact that the two frameworks securitise cyberspace by reference to different referent objects: the international order in one case, domestic public security in the other.

The negotiation process and its controversies

The Hanoi Convention's negotiating history illustrates a pattern that is central to this article's argument. The content of international instruments governing cyberspace is shaped not only by states' strategic interests but also by the design choices and business interests of technology companies, and by the advocacy of civil society organisations that understand the technical realities of how platforms operate. The Russian Federation and several other states sought a broad convention that would address not only cyber-dependent crimes but also a wide range of online content they characterise as harmful, alarming human rights organisations and technology companies alike.²⁴ The negotiating history cannot be understood without accounting for the lobbying of major technology companies concerned about data localisation requirements and government access to user data stored in their infrastructure.

24 On the negotiating history of the United Nations Convention against Cybercrime and the role of civil society and technology companies in shaping its scope, see: United Nations Office on Drugs and Crime, "Ad Hoc Committee – Home," accessed 27 August 2026, https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home.

The governance gap – where the two frameworks do not meet

Attribution, evidence, and the state/crime boundary

Perhaps the most consequential gap between the two frameworks concerns the attribution problem.²⁵ Both presuppose the ability to attribute malicious cyber conduct to a responsible actor, whether a state or an individual. In practice, attribution in cyberspace is technically complex, politically contested, and legally uncertain. The Global Mechanism has addressed attribution primarily through confidence-building measures. The Hanoi Convention addresses it through mutual legal assistance for forensic investigation. Neither framework creates binding obligations for states to share attribution findings, nor provides a mechanism for adjudicating attribution disputes.

The most significant cyber incidents of the past decade, including the attacks attributed to Russian state-sponsored groups on Ukrainian critical infrastructure and the NotPetya malicious software (malware) deployment, fall into the space between the two frameworks. They involve state or state-sponsored actors engaged in conduct that also constitutes cybercrime under national law. For such conduct, neither the Global Mechanism's voluntary norms nor the Hanoi Convention's mutual legal assistance provisions provide adequate governance tools.²⁶

The ICC's bridging attempt

The ICC Office of the Prosecutor's December 2025 Policy on Cyber-Enabled Crimes represents an important, if partial, attempt to bridge the gap between the international security framework and the criminal law framework. The policy affirms that crimes within the ICC's jurisdiction can be committed or facilitated by cyber means and explicitly applies the Rome Statute's technology-neutral provisions to the cyber domain.

- 25 On the technical, political and legal difficulties of attribution in cyberspace, see: Thomas Rid, and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38, No. 1–2 (2025): 4–37; Erik Gartzke, Jon R. Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace," *Security Studies* 24, No. 2 (2015): 316–348; Kello, *The Virtual*.
- 26 Joyce Hakmeh, and Harriet Moynihan, *Holding State-Sponsored Hackers and Other Cyber Proxies to Account: Lessons from Tackling Proxies in Russia's War on Ukraine* (London: Chatham House, 2026).

It also acknowledges the potential intersection between cyber-enabled international crimes and conduct amounting to serious crimes under national law, creating space for cooperation between the ICC and national jurisdictions.²⁷

Significantly, the policy also explicitly addresses the role of corporations. It notes that corporations may have capabilities and information which could significantly assist the investigation and prosecution of international crimes within the jurisdiction of the Court, and that corporations also have responsibilities to avoid infringing human rights. The corporate accountability dimension – unusual in an ICC policy document – reflects an implicit acknowledgement that major technology companies are not merely passive conduits for criminal conduct but active participants in the information environment within which such conduct occurs.²⁸

Structural divergences

Table. Structural Differences between the UN Global Mechanism on Cybersecurity and the UN Convention against Cybercrime

Dimension	Global Mechanism	Hanoi Convention
Primary subject	state behaviour in cyberspace	cybercrime by individuals/groups
Legal character	soft law, voluntary norms	binding treaty, legal obligations
Enforcement	none (political costs)	mutual legal assistance, domestic prosecution
Private actor role	stakeholder in DTGs	Subject of investigation / data provider
Attribution	CBMs, political statements	forensic MLA, domestic investigation
Relationship to ihl	affirmed applicable; unclear	not directly addressed
Corporate accountability	emerging; referenced in ICC policy	limited; data access provisions

Source: own analysis

These divergences are not in themselves surprising; different multilateral instruments address different problems. What is notable is the absence

²⁷ International Criminal Court, *Policy*.

²⁸ *Ibidem*.

of any formal mechanism for coordination between the two frameworks, and the degree to which the private actors who shape the technological environment in which both operate remain structurally marginal to both.

Technology companies as norm co-authors

The standard account and its limits

The standard account of international norm-making in cyberspace identifies three categories of actors: states, which negotiate and adopt international agreements; international organisations, which provide fora and administrative support; and civil society organisations and academic experts, who contribute expertise and advocacy. Technology companies appear in this account primarily as objects of regulation, entities whose products and services create the problems that states and international organisations must address. This account is increasingly inaccurate. Critical scholarship on multi-stakeholder governance has long argued that the formal architecture of intergovernmental processes can obscure the substantive co-authorship of norms by private actors, and that the multi-stakeholder model can function as either a genuine power-sharing arrangement or a fiction that legitimises corporate influence without subjecting it to political accountability.²⁹

One might object that securitisation theory in the Copenhagen School tradition is concerned with rhetorical speech acts by states or political elites and therefore cannot be straightforwardly extended to corporations. This objection has merit but it underestimates the extent to which contemporary securitisation depends on technical authority.

Where the threat being constructed is itself technical – vulnerabilities in cloud infrastructure, supply chain attacks, AI-enabled disinformation – the actors who possess the descriptive vocabulary and operational capacity to define the threat are not states but the companies. The securitising move is therefore co-produced: states make the formal political claim,

29 On critical perspectives on multi-stakeholder governance, see: Mark Raymond, and Laura DeNardis, "Multistakeholderism: Anatomy of an Inchoate Global Institution," *International Theory* 7, No. 3 (2015): 572–616; Jeanette Hofmann, "Multi-Stakeholderism in Internet Governance: Putting a Fiction into Practice," *Journal of Cyber Policy* 1, No. 1 (2016): 29–49.

but its content is supplied by corporate technical reporting. This is what Buzan, Waever and de Wilde call functional actors – entities that significantly affect decisions in the field of security without themselves being the securitising actor or the referent object.³⁰ The cyber domain blurs that distinction because the functional actor's technical authority is constitutive of the threat construction.

The role of technology companies in international norm-making can therefore be interpreted within a broader theoretical shift in international relations. Contemporary security competition increasingly takes place in domains that are not fully controlled by states, including cyberspace, digital infrastructure, and global data flows.³¹ In such conditions, private actors that control technological platforms may acquire forms of influence traditionally associated with state power. The participation of technology companies in cybersecurity governance should therefore not be treated as an anomaly but rather as a structural feature of contemporary international politics in which technological capability functions as a key source of authority.

Infrastructure as normative choice

The most fundamental way in which technology companies participate in norm-making is through their infrastructure decisions. The architecture of the internet – its routing protocols, encryption standards, and platform designs – embeds normative choices about privacy, surveillance, access, and control. These choices are made by engineers and product managers at private companies, often without meaningful democratic deliberation and frequently with consequences that extend across jurisdictions and affect the strategic capabilities of states.³²

30 Buzan, Waever, and de Wilde, *Security*: 35–42.

31 On the growing role of non-state actors and technological power in contemporary security governance, see: Ronald J. Deibert, *Black Code: Surveillance, Privacy, and the Dark Side of the Internet* (Toronto: Signal, 2013); Lennart Maschmeyer, *Subversion: Technology, the Internet, and the Logic of Modern Political Violence* (Oxford: Oxford University Press, 2022).

32 Laura DeNardis, *The Global War for Internet Governance* (New Haven: Yale University Press, 2014); Joseph S. Nye, *The Future of Power* (New York: Public Affairs, 2011).

The decision by major cloud providers about where to locate data centres, and under what legal conditions to respond to government requests for access to data stored in them, shapes the practical operation of both the Global Mechanism's confidence-building measures and the Hanoi Convention's mutual legal assistance provisions. A state party to the Hanoi Convention seeking assistance from another party in accessing data stored by a US-based cloud provider will find that the effective legal framework governing that access is determined at least as much by the company's terms of service and internal compliance policies as by the Convention's MLA provisions.

Participation in forum design

Beyond their infrastructural role, technology companies increasingly participate in multilateral policy processes related to cybersecurity. The ICC cyber policy's acknowledgement that its January 2024 conference examining the implications of cyberspace misuse was organised in partnership with Microsoft illustrates a broader pattern of structured engagement between international institutions and major technology firms. This engagement takes multiple forms, including funded partnerships, secondments, expert consultations, and participation in multi-stakeholder policy discussions.

The negotiating history of the UN Convention against Cybercrime provides another example of this dynamic. Concerns expressed by technology companies regarding encryption obligations and data-access requirements influenced debates on procedural safeguards and the balance between law-enforcement powers and privacy protections. Rather than operating outside multilateral processes, private actors increasingly participate within them, even though their influence is not always visible in the formal legal structure of the resulting instruments.

The Global Mechanism's approach and its limits

The Global Mechanism's approach to private actor involvement is more structured but also more limited. This limitation is particularly visible in the final report of the Open-Ended Working Group, which emphasises continuity, institutional structure, and intergovernmental decision-making rather than a transformation of the governance model.³³ The future permanent mechanism is explicitly framed as a continuation of the OEWG

33 United Nations General Assembly, *Final Report of the Open-ended*, 2025.

process rather than a fundamentally new institutional design, which reinforces the intergovernmental character of the framework despite the growing importance of private technological actors. The report does provide for engagement with other stakeholders, including private sector actors and technical experts, but this participation is framed as consultative rather than constitutive of the decision-making process.

This formal intergovernmentalism coexists with a substantive reality in which the most consequential decisions about the security of critical infrastructure are made by companies rather than governments. The DTGs can discuss critical infrastructure protection, but they cannot compel the companies that own and operate much of that infrastructure to implement protective measures.³⁴

Recommendations

As mentioned in section 1.1, the OSCE confidence-building framework serves as a comparative reference point because it is the most institutionally developed regional analogue to the Global Mechanism. The OSCE's long engagement with cybersecurity – including its pioneering work on confidence-building measures, its dense network of participating States spanning North America, Europe, and Central Asia, and its political format that includes both NATO and CSTO members – offers operational lessons that purely conceptual analysis of the UN process cannot provide. Three thematic clusters emerge.

Bridging the security-criminal law divide

Experience from the OSCE confidence-building framework suggests that the institutional separation between international security discussions and criminal law cooperation can be mitigated through operational rather than purely normative mechanisms. The OSCE model emphasises structured exchanges between national authorities responsible for cybersecurity policy, incident response, and law-enforcement cooperation, particularly through confidence-building measures focused on consultation, information exchange, and institutional contact points.

34 United Nations General Assembly, *Developments*, 2025; Rupp, *The UN's*.

The first lesson concerns the need for procedural bridges between national Computer Emergency Response Teams (CERTs), law-enforcement authorities, and foreign-policy structures. Many significant cyber incidents simultaneously implicate issues of state responsibility, criminal liability, and critical-infrastructure protection. The OSCE experience shows that information-sharing mechanisms designed solely for technical incident response or solely for criminal investigation are insufficient. More effective responses depend on coordinated national structures capable of transferring information rapidly between these domains and engaging in structured consultations with other states when incidents risk escalation.³⁵

Secondly, the OSCE framework demonstrates the value of institutionalised dialogue in situations where legal qualification remains uncertain. Confidence-building measures encouraging consultations and the use of designated points of contact provide a procedural mechanism through which states can clarify incidents without immediately framing them in terms of legal responsibility. This approach is particularly relevant in cases where the same conduct may simultaneously constitute a cyber-crime, a breach of international law, or a violation of voluntary norms of responsible state behaviour.

Finally, OSCE practice illustrates that capacity-building measures play a critical role in bridging the security-criminal law divide. Training programmes, expert exchanges, and shared terminology initiatives strengthen states' ability to interpret international legal obligations consistently while improving the effectiveness of domestic investigative and cooperative frameworks. The Global Mechanism could benefit from adopting similar cross-sectoral capacity-building initiatives.

Formalising corporate accountability in multilateral frameworks

The OSCE experience also offers a structured model for integrating private actors into international cybersecurity governance without undermining the intergovernmental character of the process. Several OSCE confidence-

35 Organization for Security and Co-operation in Europe, *Initial Set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies*, 2013; Organisation for Security and Co-operation in Europe, *OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies*, 2016.

-building measures implicitly recognise that the effective implementation of cyber-related obligations depends on cooperation with private-sector entities that operate critical infrastructure, provide digital services, and control access to relevant data.

Confidence-building measures relating to cross-border cooperation, public-private partnerships, and critical-infrastructure protection assume an institutional role for companies that goes beyond the traditional conception of corporations as mere objects of regulation. Effective implementation of cybercrime conventions, international accountability mechanisms, and incident-response frameworks depends on sustained cooperation with private actors that possess both the technical expertise and the operational control necessary to detect, attribute, and mitigate cyber operations.

The OSCE approach suggests that the role of companies should be formalised rather than treated as ad hoc participation. This could include structured consultation mechanisms within the Global Mechanism's thematic working groups, voluntary transparency frameworks concerning government data-access requests, and agreed standards for corporate participation in incident-response coordination. Such mechanisms would not transform companies into formal subjects of international law, but they would acknowledge their practical role as co-producers of security outcomes in cyberspace.³⁶

Attribution and accountability without escalation

A third lesson derived from the OSCE context concerns the relationship between attribution and escalation. The OSCE confidence-building measures emphasise procedural transparency, structured consultations, and reliable communication channels as mechanisms designed to reduce the risk that cyber incidents will generate misperception or political overreaction.

Rather than treating attribution primarily as a question of public political statements, the OSCE framework promotes a gradual and procedural approach based on technical information-sharing, consultations among designated national points of contact, and the use of established communication channels before formal accusations are made. This approach reflects

36 Organisation of Security and Co-operation in Europe, *Initial*; Organisation of Security and Co-operation in Europe, *OSCE*; Organisation of Security and Co-operation in Europe, *Guide on Developing National Cybersecurity Strategies*, 2013.

an implicit recognition that attribution in cyberspace is rarely purely technical and that premature political attribution can contribute to escalation even where the underlying facts remain uncertain.

For the Global Mechanism, the key lesson is that accountability mechanisms should not rely exclusively on public attribution or formal legal responsibility. They should incorporate graduated procedures that allow states to clarify incidents, exchange information, and manage disputes without immediately escalating them into legal or political confrontation. Such an approach would strengthen the credibility of the framework for responsible state behaviour while preserving the stability that confidence-building measures are designed to promote.³⁷

Conclusions

The launch of the UN Global Mechanism in March 2026, together with the parallel development of the Hanoi Convention, represents a significant stage in the long process through which cyberspace has been constructed as a domain of international security. The analysis developed in this article suggests that the emergence of parallel governance frameworks in cyberspace should be understood not only as an institutional but also a theoretical problem. The coexistence of soft-law security mechanisms, binding criminal-law instruments, and informal corporate influence reflects a broader transformation of the international system in which the production of norms is no longer monopolised by states. International law in the digital domain develops at the intersection of geopolitical competition, technological innovation, and transnational corporate power.

From this perspective, the distinction between state behaviour in cyberspace and cybercrime is not merely a technical or legal differentiation but a product of the way different actors seek to define the nature of the threat. The Global Mechanism reflects the securitisation of cyberspace as an issue of international peace and security, while the Hanoi Convention reflects its securitisation as a transnational criminal threat. The coexistence of these two frameworks therefore illustrates not only institutional fragmentation but also competing securitising narratives about what cyberspace is and

37 Organisation for Security and Co-Operation in Europe, *OSCE*; United Nations, *Report of the Group of Governmental Experts*, 2021.

why it matters.³⁸ In this sense, the development of international law norms in cyberspace can itself be understood as a securitising move: intergovernmental organisations such as the UN co-produce the construction of cyberspace as an existential threat domain through the very process of norm-making, while corporate actors supply the technical content that makes such claims credible.

The role of technology companies further demonstrates the limits of a purely state-centred model of securitisation. The actors that possess the greatest technical capacity to identify, attribute, and mitigate cyber operations are not states but private companies that design and operate the digital infrastructure on which both security and criminal investigations depend. As a result, securitisation in the cyber domain increasingly depends on the authority and expertise of actors that are formally external to the traditional structures of international law.³⁹ The ICC's cyber policy of December 2025 is particularly significant in this respect. It implicitly recognises that the effectiveness of international legal accountability in cyberspace depends on cooperation with the private sector.

The Global Mechanism's Dedicated Thematic Groups offer an opportunity to move beyond a purely rhetorical form of securitisation towards a more coherent governance framework. Whether this opportunity will be used depends on decisions that remain unresolved at the time of writing, particularly those concerning expertise, agenda-setting, and the relationship between technical knowledge and diplomatic negotiation. The role of European actors in shaping these decisions is likely to be important, especially if grounded not only in regulatory experience but also in a more explicit recognition of how technological power reshapes the process through which security threats are defined.

The central challenge of cybersecurity governance in 2026 is therefore not only institutional but conceptual. This reflects a broader shift already identified in the literature on cyber norms, which recognises non-state actors as increasingly important contributors to the formation of customary standards of responsible behaviour in cyberspace.⁴⁰ The process analysed in this

38 Buzan, Waever, and de Wilde, *Security*: 23–26.

39 Kulesza and Eggenschwiler, *Non-State*: 245–262.

40 Finnemore and Hollis, *Constructing*: 425–479; Kulesza and Eggenschwiler, *Non-State*: 245–262.

article suggests that cybersecurity is no longer simply a technical problem or a legal one. It has become a central object of securitisation in contemporary international relations, in which threats are constructed through discourse, legitimised through institutional innovation, and managed through a complex interaction between states, international organisations, and private technological actors.⁴¹ The evolution of cybersecurity governance illustrates a broader transformation of international security in which the construction of threats increasingly takes place in the informational and technological domain rather than exclusively in the military sphere.

Bibliography

- Buzan, Barry, Ole Wæver, and Jaap de Wilde. *Security: A New Framework for Analysis*. Boulder: Lynne Rienner, 1998.
- Council of Europe. *Convention on Cybercrime*. 2001.
- Deibert, Ronald J. *Black Code: Surveillance, Privacy, and the Dark Side of the Internet*. Toronto: Signal, 2013.
- DeNardis, Laura. *The Global War for Internet Governance*. New Haven: Yale University Press, 2014.
- Baele, Stephane, and Thomson Catarina. "Securitisation Theory." In *Contemporary Security Studies*, edited by Alan Collins. Oxford: Oxford University Press, 2018.
- Finnemore, Martha, and Duncan B. Hollis. "Constructing Norms for Global Cybersecurity." *American Journal of International Law* 110 (2016).
- Gartzke, Erik, and Jon R. Lindsay. "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace." *Security Studies* 24, No. 2 (2015).
- Hakmeh, Joyce, and Harriet Moynihan. *Holding State-Sponsored Hackers and Other Cyber Proxies to Account: Lessons from Tackling Proxies in Russia's War on Ukraine*. London: Chatham House, 2026.
- Hofmann, Jeanette. "Multi-Stakeholderism in Internet Governance: Putting a Fiction into Practice." *Journal of Cyber Policy* 1, No. 1 (2016).
- International Criminal Court, *Policy on Cyber-Enabled Crimes under the Rome Statute*. 2025.
- Kello, Lukas. *The Virtual Weapon and International Order*. New Heaven: Yale University Press, 2017.

41 On securitisation as a co-produced process involving intergovernmental organisations and non-state actors, see: Buzan, Waever, and de Wilde, *Security*: 21–26; Stephane Baele, and Catarina Thomson, "Securitisation Theory," in *Contemporary Security Studies*, ed. Alan Collins (Oxford: Oxford University Press, 2018).

- Klotz, Audie, and Deepa Prakash, eds. *Qualitative Methods in International Relations: A Pluralist Guide*. Basingstoke: Palgrave Macmillan 2008.
- Kulesza, Joanna, and Jacqueline Eggenschwiler. "Non-State Actors as Shapers of Customary Standards of Responsible Behavior in Cyberspace." In *Governing Cyberspace: Behavior, Power and Diplomacy*, edited by Dennis Broeders, Bibi van den Berg. London: Rowman & Littlefield International, 2020.
- Lewis, James Andrew. *Creating Accountability for Global Cyber Norms*. Washington: Center for Strategic and International Studies, 2022. Accessed 16 June 2026. <https://www.csis.org/analysis/creating-accountability-global-cyber-norms>.
- Maschmeyer, Lennart. *Subversion: Technology, the Internet, and the Logic of Modern Political Violence*. Oxford: Oxford University Press, 2022.
- Maurer, Tim. *Cyber Norms: Why International Cooperation on Cybersecurity Is Failing*. New York: Council on Foreign Relations, 2011.
- Nye, Joseph S. *The Future of Power*. New York: Public Affairs, 2011.
- Nye Joseph S. Jr. *The Regime Complex for Managing Global Cyber Activities*. Waterloo and London: Centre for International Governance Innovation and Chatham House, 2014.
- Organization for Security and Co-operation in Europe. *Initial Set of OSCE Confidence Building-Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies*. 2013.
- Organization for Security and Co-operation in Europe. *OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies*. 2016.
- Organization for Security and Co-operation in Europe. *Guide on Developing National Cybersecurity Strategies*. 2013.
- Pytlak, Allison, Christina Rupp, Eugene Tan, Louise Marie Hurel, Talita Dias, and Valentin Weber. *The Rules of the Road in Cyberspace, 10 Years Later*. London: Royal United Services Institute, 2025.
- Raymond, Mark and Laura DeNardis. "Multistakeholderism: Anatomy of an Inchoate Global Institution." *International Theory* 7, No. 3 (2015).
- Republic of France. *Programme of Action (PoA) to Advance Responsible State Behaviour in the Use of ICTs in the Context of International Security*. 2023.
- Rid, Thomas, and Ben Buchanan. "Attributing Cyber Attacks." *Journal of Strategic Studies* 38, No. 1-2 (2015).
- Risse, Thomas, ed. *Governance without a State? Policies and Politics in Areas of Limited Statehood*. New York: Columbia University Press 2011.
- Rosenau, James. *Along the Domestic-Foreign Frontier: Exploring Governance in a Turbulent World*. Cambridge: Cambridge University Press, 1997.
- Rupp, Christina. *The UN's New Global Mechanism on Cybersecurity: How Europe Can Advance Responsible State Behaviour in Cyberspace*. Berlin: Interface, 2026.
- Schmitt, Michael, ed. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, 2017.

- Slaughter, Anne-Marie. *A New World Order*. Princeton: Princeton University Press, 2004.
- United Nations General Assembly. *Developments in the Field of Information and Telecommunications in the Context of International Security*. 1998.
- United Nations, *Convention against Cybercrime*. 2024.
- United Nations General Assembly. *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*. 2021.
- United Nations General Assembly. Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025. *Final Report of the Open-Ended Working Group*. 2025.
- United Nations General Assembly. *Developments in the Field of Information and Telecommunications in the Context of International Security. Note by the Secretary-General Transmitting the Final Report of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025*. 2025.
- United Nations Office on Drugs and Crime. “Ad Hoc Committee – Home.” https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home.