GLOBAL INITIATIVE
AGAINST TRANSNATIONAL ORGANIZED CRIME

WHOSE TREATY IS IT ANYWAY?

THE PRESENT AND FUTURE OF THE UN CYBERCRIME CONVENTION

Ian Tennant | Helena Yixin Huang

SEPTEMBER 2026

ACKNOWLEDGEMENTS

The authors would like to thank the Global Initiative Against Transnational Organized Crime (GI-TOC) Publications team for all their hard work, and with special thanks to Aden Rapanos, who carried out vital research for the publication during his internship at the GI-TOC.

ABOUT THE AUTHORS

Ian Tennant is the Director of Multilateral Engagement at the GI-TOC, and has been monitoring and engaging closely with the negotiations towards a cybercrime treaty over several years.

Helena Yixin Huang is a cybercrime researcher based in Singapore. Her views in this policy piece are her own and do not represent the official position of any organizations she is or might be associated with.

Cover: © *Daniel Slim/AFP via Getty Images*

Please direct inquiries to:
The Global Initiative Against Transnational Organized Crime
Avenue de France 23
Geneva, CH-1202
Switzerland
www.globalinitiative.net

CONTENTS

Summary 1

Key findings 1

Introduction: the road to consensus 3

Reconciling different perspectives 6

Translating the provisions into practice 9

From information silos to shared intelligence 9

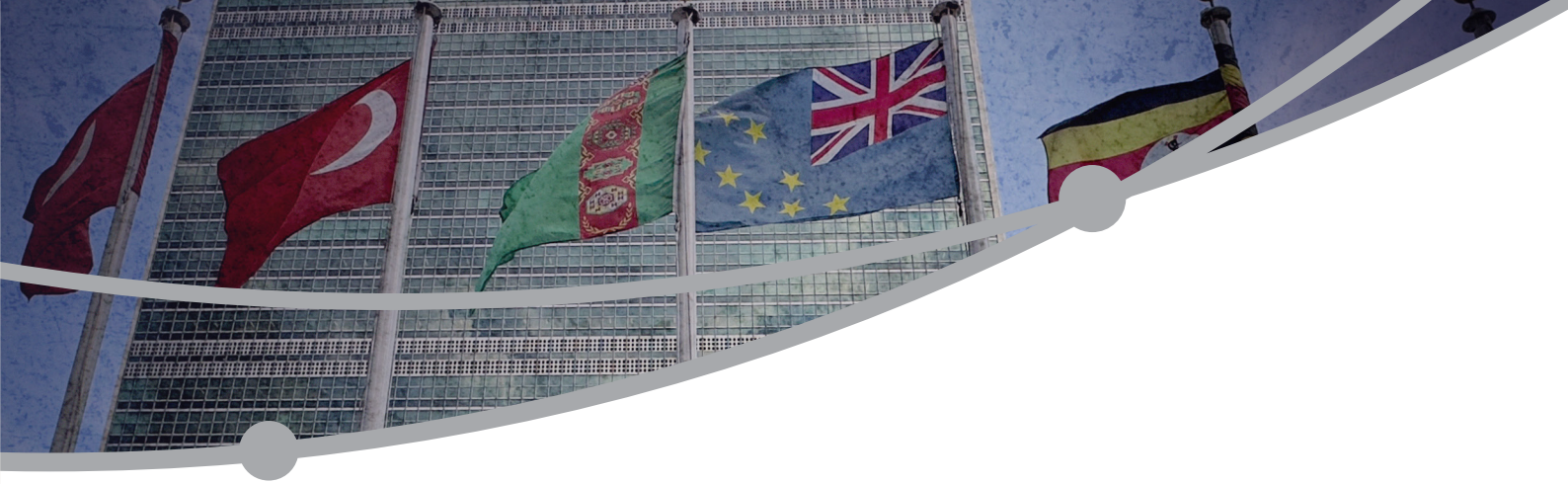
Aligning systems for operational readiness 11

Building trust through predictability and safeguards 12

Including multi-stakeholders in implementation 14

Conclusion 17

Notes 18



SUMMARY

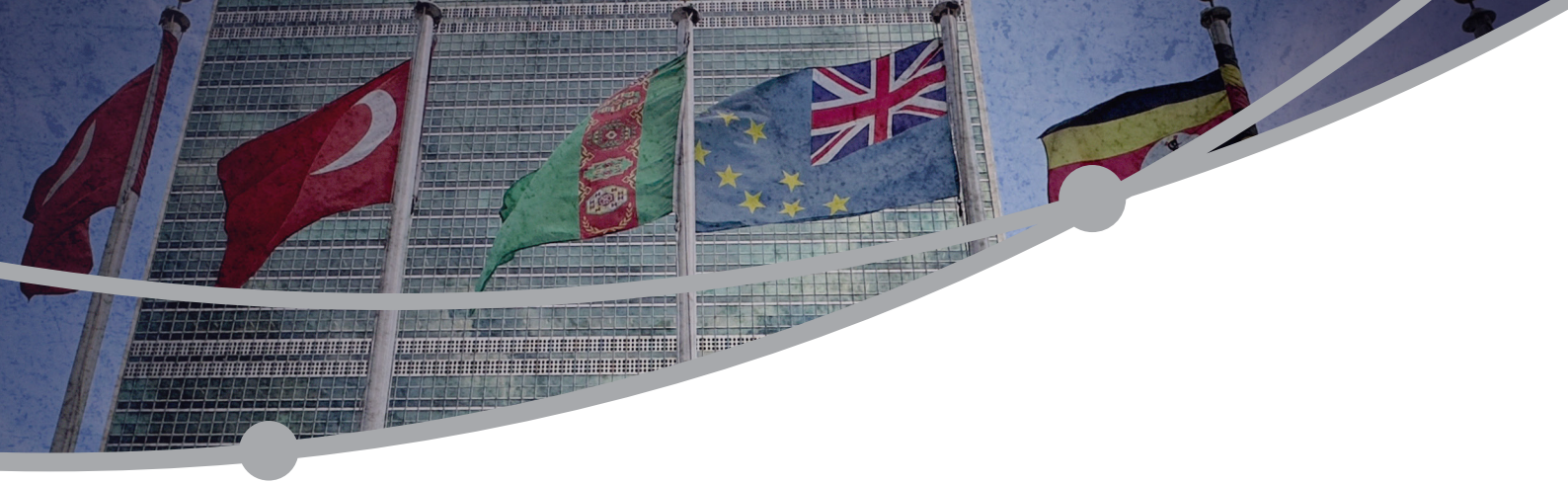
The United Nations Convention against Cybercrime (Hanoi convention) is a widely signed new legal instrument that was agreed by consensus at a time of geopolitical fragmentation. The potential benefits of the convention are considerable, as are the potential risks if it is misused. This policy brief reviews the history and content of the convention and considers its future, concluding that cross-regional and cross-sectoral trust building and engagement will be essential for its success.

But whose treaty is it? The convention is no longer owned by those who proposed it, nor by those who initially rejected it. Its history has been marked by polarization and suspicion, but its future must be one of shared ownership – by the states parties, coming from different perspectives, as well as by the private sector and civil society, who recognize the unique role they play in implementation, all under the auspices of the UN.

Key findings

- The ecosystem of cyber-dependent and cyber-enabled crime is both transnational and highly adaptive, making it increasingly difficult for states to respond through isolated or purely domestic measures.
- There has never been a consensus on the need for a new UN treaty, but member states have overcome their differences to reach a consensus on this treaty, the terms of which are based on overarching human rights safeguards.
- Despite member state consensus, there are some countries that want to expand the treaty's scope through new supplementary protocols (led by Russia), and others that do not look like they will sign up – including the US, where major technology companies are based.
- Many of those big technology companies, along with human and digital rights NGOs, are vocally opposed to the treaty. Other civil society experts are hopeful that it will have an impact against harmful and exploitative forms of criminality carried out online.
- Law enforcement organizations are clear on the benefits of the treaty, in the context of fragmented and disparate domestic and international frameworks.
- Countries in the Global South have strongly advocated for more capacity building and technical assistance, and are hoping for a treaty that can deliver, but politics and financial resource constraints do not bode well.

- The convention references non-governmental stakeholders many more times and in many more contexts than the existing UN counter-crime conventions, which augurs well for an effective and open implementation process, but this engagement must be built on trust.
- At the operational level, building trust through predictability, safeguards and institutional networking and capacity building will be key to the treaty's success.
- At the political level, states parties must build trust through an open and inclusive engagement mechanism, in recognition of the broad and deep roles of diverse stakeholders throughout the convention.



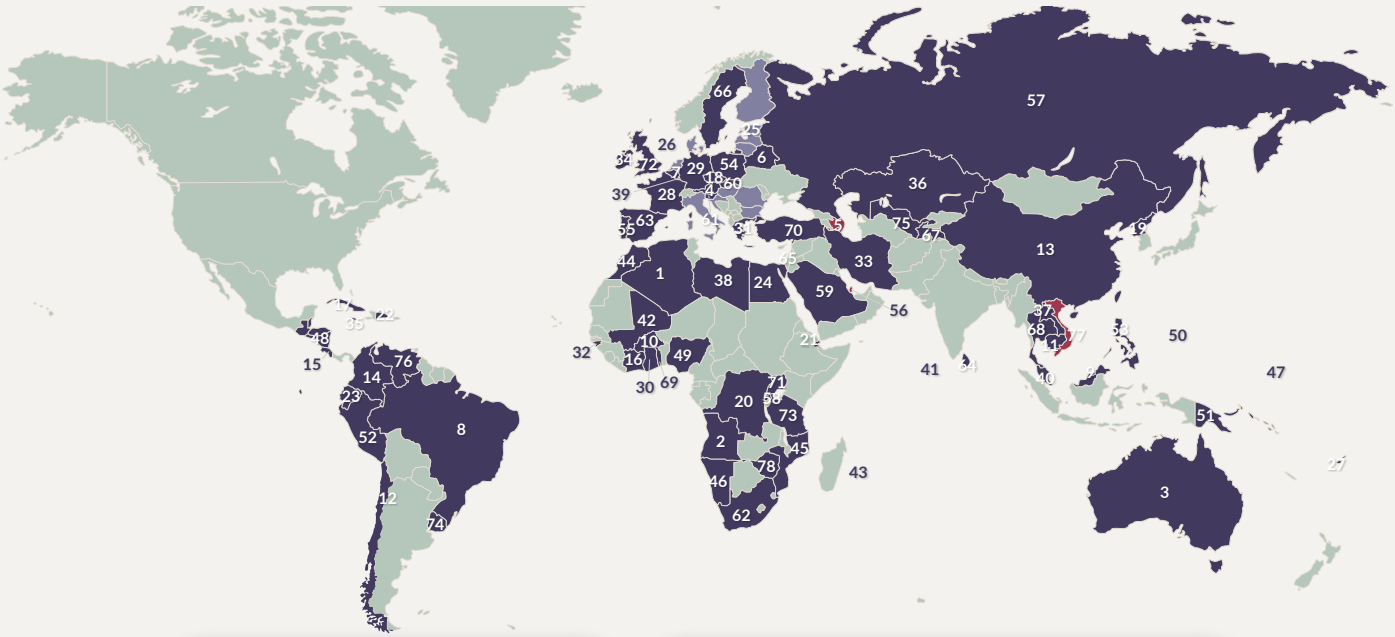
INTRODUCTION: THE ROAD TO CONSENSUS

The adoption by consensus of the UN Convention against Cybercrime at the General Assembly in October 2025, and its subsequent signing in Hanoi by 75 member states, was a significant milestone that was by no means inevitable.[1] The convention's development phase was characterized by a lack of common understanding or shared vision. Even before the more recent geopolitical division emerged, there was a clear and deep divide between those who were pushing for the convention – mainly Russia and China – and those in the West who opposed it. These divisions were clear throughout all the negotiations on the convention but were eventually overcome. Indeed, the convention already has its first parties: Qatar, which acceded in February 2026, and Azerbaijan and Vietnam, which adopted it in April.[2]

The need for a universally accepted global framework for combating cybercrime was urgent. Cyber-related crimes continue to expand in scale, complexity and geographic distribution, affecting both source and target countries.[3] However, the current legal frameworks are not being implemented effectively enough to reduce cybercriminal activity,[4] and capacity is weak in many jurisdictions. INTERPOL estimates that the total value lost to cybercrime yearly rivals the GDPs of major economies.[5]

The term 'cybercrime' encompasses activities that range from financially motivated scams and ransomware attacks to cyber-enabled trafficking and illicit online marketplaces. These activities are often interconnected,[6] with proceeds from one form of criminal activity being reinvested into others. The resulting ecosystem is not only transnational but also highly adaptive, making it increasingly difficult for states to respond through isolated or purely domestic measures.

The cybercrime convention represents an international effort, under the auspices of the UN, to establish a global baseline for the criminalization of cybercrime and the facilitation of cross-border cooperation. It is designed to complement existing regional instruments, such as the Budapest Convention on Cybercrime, which was created by the Council of Europe in 2001 (and has been in force since 2004). The Budapest convention is aimed at addressing internet and computer-related crime and has served as a foundational framework for international cooperation among its signatories. However, its reach remains limited because of uneven adoption and varying levels of engagement by states.



Once 40 signatories become states parties, the treaty will enter into force. This could happen in 2027.

The European Union as a whole is a signatory and will become a party in its own right once the first member state of the EU becomes a state party.

States parties | Signatory states | Signatory regional economic integration organization

1. Algeria
2. Angola
3. Australia
4. Austria
5. Azerbaijan
6. Belarus
7. Belgium
8. Brazil
9. Brunei Darussalam
10. Burkina Faso
11. Cambodia
12. Chile
13. China
14. Colombia
15. Costa Rica
16. Côte d'Ivoire
17. Cuba
18. Czech Republic
19. Democratic People's Republic of Korea
20. Democratic Republic of the Congo
21. Djibouti
22. Dominican Republic
23. Ecuador
24. Egypt
25. Estonia
26. European Union
27. Fiji
28. France
29. Germany
30. Ghana
31. Greece
32. Guinea-Bissau
33. Iran (Islamic Republic of)
34. Ireland
35. Jamaica
36. Kazakhstan
37. Lao People's Democratic Republic
38. Libya
39. Luxembourg
40. Malaysia
41. Maldives
42. Mali
43. Mauritius
44. Morocco
45. Mozambique
46. Namibia
47. Nauru
48. Nicaragua
49. Nigeria
50. Palau
51. Papua New Guinea
52. Peru
53. Philippines
54. Poland
55. Portugal
56. Qatar
57. Russian Federation
58. Rwanda
59. Saudi Arabia
60. Slovakia
61. Slovenia
62. South Africa
63. Spain
64. Sri Lanka
65. State of Palestine
66. Sweden
67. Tajikistan
68. Thailand
69. Togo
70. Türkiye
71. Uganda
72. United Kingdom of Great Britain and Northern Ireland
73. United Republic of Tanzania
74. Uruguay
75. Uzbekistan
76. Venezuela (Bolivarian Republic of)
77. Vietnam
78. Zimbabwe

FIGURE 1 Signatory states and states parties to the UN Convention against Cybercrime.

The UN Convention against Cybercrime was adopted by consensus at the General Assembly in October 2025, but the road towards its implementation remains uncertain. *Photo: UNODC*

The Hanoi convention faces similar challenges. Since its initiation by Russia, it has been the subject of intense negotiations due to disagreements over many issues, including even its title,[7] and has followed an unpredictable and fraught trajectory.[8] In effect, the convention represents a compromise between the varied positions held by different states during the negotiations and has been both criticized and supported by non-governmental players.[9]

This policy brief explores the opportunities and challenges of this convention. It examines the polarized views that characterized the negotiations and the various perspectives of the stakeholders involved in the convention's development and eventual implementation. It also outlines issues that need to be addressed if the convention is to work effectively, including how to translate its provisions into practice, and how to include diverse stakeholders in its implementation. It concludes by highlighting the importance of trust building on various levels – among practitioners, between sectors, and between different regional and political groupings. The complex range of issues and sensitivities will not be solved through narrow or closed engagement; a broad range of stakeholders are recognized in the convention itself and must be part of the solution as it moves towards implementation.

RECONCILING DIFFERENT PERSPECTIVES

Since its initiation in 2019, the UN cybercrime convention has been the subject of debate regarding both its scope and the form it should take, reflecting the divisions that exist among member states and across sectors. The negotiations were a pitched battle between the Russian vision of a form of 'internet control' treaty and the Western vision of a cooperation instrument with strong human rights safeguards. Meanwhile, countries in the Global South were keen to support any instrument that could increase cooperation and build capacity. The result is a compromise that has enjoyed broad support, without any side seeing their vision defeated, which should be seen as a sign of hope for the treaty and for future action against cybercrime. Russia and China advocated for a broad and all-encompassing treaty to criminalize, facilitate criminalization and advance international cooperation on a wide and diverse range of crimes that involve information and communications technology (ICT).[10] Supported by China and others, Russia is now pushing for a supplementary protocol to specify an additional range of criminal offences under the treaty, 'while focusing on combating the use of ICT for terrorist and extremist purposes, as well as drug and arms trafficking'.[11]

In contrast, Western countries are broadly satisfied with the convention and are concerned that any expansion of offences could result in a broad and authoritarian criminalization of everyday activities, or the exercise of rights, including private messaging through apps or social media posts.[12] Their vision was for a treaty that is focused on a specific list of cyber-dependent offences and enables states to cooperate on a broader range of crimes alongside a set of human rights and data protection safeguards. Countries such as New Zealand and Canada pushed most strongly for the overarching safeguards to protect human rights and privacy, as, in Canada's statement on the convention's adoption, 'any attempt to misuse the Convention would undermine its credibility and could constitute a violation of the Convention'.[13] Meanwhile, the US has adopted a 'wait and see' position, but no one is expecting it to join the treaty any time soon, especially considering the strong opposition to it from the private sector.[14] The signature of the European Union is noteworthy as a political statement of intent from a region that strongly supports the Budapest convention.[15]

For many countries in the Global South, the convention is an opportunity to rebalance international cooperation, which has historically centred on Western-led mechanisms, and to secure greater capacity-building support. These countries will be impatiently waiting to see whether these opportunities will come to fruition any time soon, as capacity building is considered 'a vital element in bridging the digital divide'.[16]

Timeline of the UN Convention against Cybercrime

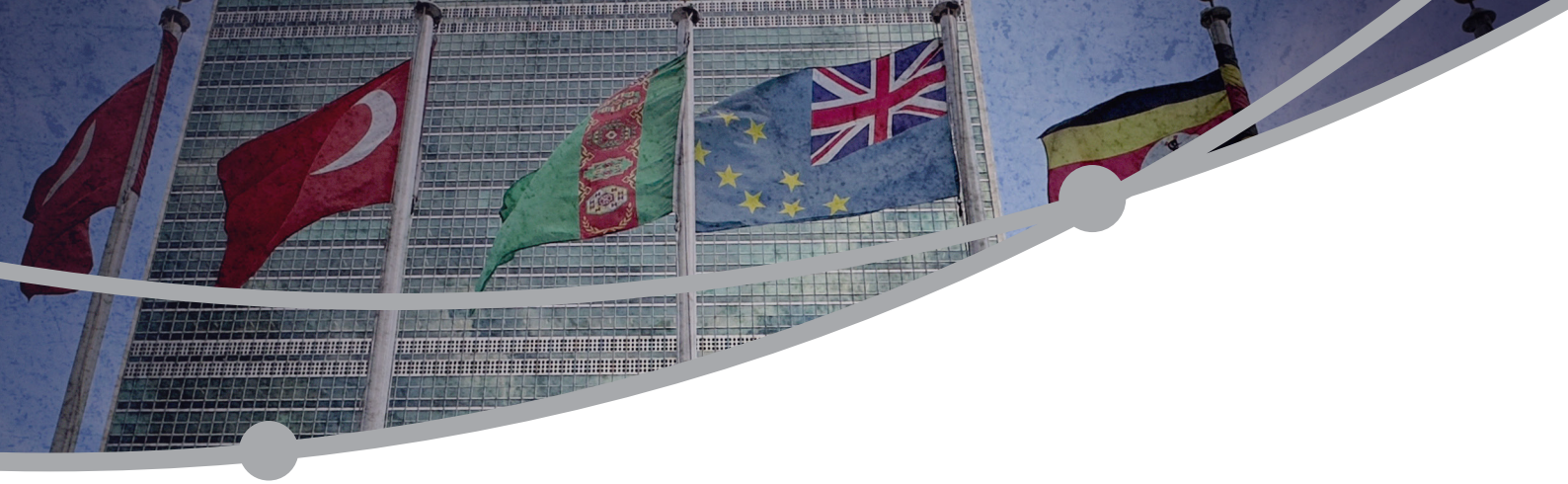
Outside government, the convention has drawn mixed but typically critical reactions. Multinational corporations – particularly those based in the US, which control most of the internet's infrastructure and, therefore, the majority of data – have been vocal in their opposition. For instance, Cisco, a leading American multinational conglomerate in the business of networking hardware, software and telecommunications equipment, believes that the convention is more focused on preventing the dissemination of 'objective information' than on 'hacking and cybercrimes' and, therefore, does not support free speech.[17] The organization's view is that the convention, in requiring companies to provide data and evidence, would increase the cost and difficulties of their operations. Going further, the Cybersecurity Tech Accord, an industry body of technology companies, has described the convention as 'a surveillance treaty'.[18] Nevertheless, parts of the private sector did participate in the negotiation process and contribute to the convention's development.

Human rights groups and data privacy organizations have been even more critical, warning that the convention could legitimize repression under the guise of cybercrime enforcement. They issued a joint statement calling on states to 'refuse to sign or ratify the Convention' and, for states that had already committed to signing, to 'adopt concrete human rights safeguards'.[19] Despite the inclusion of overarching safeguards in the final convention text, these groups argue that the risk of misuse remains

high, particularly in jurisdictions with weaker rule-of-law protections. If misuse were to happen, the convention could create a crisis of confidence in the UN, as the guardian of this instrument, given its parallel role as a standard-setter and monitor of human rights around the world.

At the same time, some civil society groups – particularly those working on safeguarding people from online abuse – see clear benefits to this latest multilateral instrument. The criminalization of offences such as the non-consensual sharing of intimate images is considered a major step forward, with the potential to 'dramatically improve how quickly and effectively victims can seek justice, especially when dealing with the borderless nature of online abuse'.[20]

There are some substantive gaps in the convention, specifically on the issue of cyber scams, which exploded as phenomenon throughout the timeline of the negotiations.[21] In addition, the treaty's potential to help address key criminal markets that rely on online marketplaces, such as wildlife trafficking and human trafficking and smuggling, has not been explored in detail.



TRANSLATING THE PROVISIONS INTO PRACTICE

Among public officials, it is law enforcement and judicial authorities who most clearly see the benefits of the cybercrime convention, particularly for building capacity, establishing connections,[22] and creating opportunities for investigations, prosecutions and international cooperation that did not exist before.

Beyond the number of signatories and ratifications, the convention's success will depend on how member states translate legal provisions into practical mechanisms for investigation, evidence sharing and enforcement. Such implementation challenges are not unique to cybercrime enforcement. Across multiple domains of transnational crime, the gap between legal commitment and operational practice has often limited the effectiveness of international agreements.[23] In the cybercrime context, this gap is further complicated by the speed of technological change and the inherently transnational nature of digital activity, while the diversification of cybercrime has further complicated coordination efforts.

In light of this, implementation of the cybercrime convention will require a proactive strategy to address the structural gaps that continue to hinder global responses. These can be broadly categorized into three interrelated pillars: knowledge, capacity and trust. Each of these pillars reflects a different dimension of the implementation challenge, and all three must be addressed concurrently if the convention is to function as an effective operational instrument rather than remain a symbolic legal framework.

From information silos to shared intelligence

The knowledge gap could be reduced through more systematic and coordinated information sharing. In traditional cybersecurity and law enforcement contexts, information is often restricted on a need-to-know basis to protect confidentiality and system integrity.[24] Although this approach is necessary in certain operational settings, it is less effective when it comes to cybercrime ecosystems, which often exploit fragmentation and asymmetries in information.[25]

Cybercrime operations are increasingly structured, adaptive and transnational, relying on distributed infrastructures, such as malware development networks, anonymized communication channels and complex financial flows. In such an environment, no single organization or jurisdiction is likely to possess a complete view of the threat landscape. Intelligence on fraud patterns, ransomware infrastructure

and financial flows is often distributed across telecommunications providers, financial institutions, cybersecurity firms and law enforcement agencies. This fragmentation is not only institutional but also functional, as different actors possess distinct categories of intelligence:

- At a tactical level, organizations may identify indicators of compromise, such as IP addresses, malware signatures and phishing domains.
- At an operational level, law enforcement agencies may observe recurring tactics, techniques and procedures associated with particular threat actors.
- At a strategic level, policymakers and researchers may distinguish broader trends, including the emergence of crime-as-a-service models and the convergence of cybercrime with other forms of organized crime.

Without mechanisms that can integrate these layers of intelligence, responses are more likely to remain reactive and incident driven, limiting the ability of authorities to identify patterns, anticipate emerging threats and disrupt criminal networks. The challenge is further compounded by differences in how cybercrime data is classified and interpreted across jurisdictions. Variations in terminology, reporting standards and thresholds for what constitutes an act of cybercrime can limit the comparability of data and hinder collective analysis. Without a degree of alignment in how cyber incidents are defined and recorded, efforts to build a shared understanding of the threat landscape may remain incomplete. This has implications not only for operational responses, but also for policy development, resource allocation and long-term strategic planning.

This can be observed in approaches towards ransomware investigations,[26] where elements of the attack infrastructure, including command-and-control servers, cryptocurrency wallets and malware variants, are often identified by different entities across jurisdictions. In several publicly reported cases involving ransomware groups, such as Russia-based REvil and Conti,[27] delays or gaps in consolidating threat intelligence across stakeholders appear to have coincided with the reuse of infrastructure and the replication of attack patterns across multiple targets.

The growth of crime-as-a-service ecosystems further underscores this issue. Services such as phishing kits, ransomware-as-a-service platforms and access brokers enable actors with varying levels of technical expertise to participate. These ecosystems develop rapidly, with tools and services frequently modified and redistributed. Without timely sharing of relevant intelligence, enforcement efforts may struggle to keep pace with these developments.

Therefore, the effective implementation of the cybercrime convention requires a calibrated shift towards a need-to-share approach. This is broadly aligned with the convention's provisions on international cooperation and information exchange, including those that encourage collaboration in the prevention, detection and investigation of cybercrime. The objective is not indiscriminate disclosure, but the structured sharing of non-sensitive technical indicators, aggregated data and analytical insights to support a more comprehensive understanding of the threat landscape.

Large-scale scam operations in South East Asia provide an illustrative example.[28] In multiple jurisdictions, industrialized scam networks involving online fraud and human trafficking operated over extended periods before coordinated enforcement actions were undertaken. These networks were identified by non-governmental actors, including civil society organizations and investigative journalists, not by law enforcement channels, suggesting that gaps in integrating information may delay recognition of emerging criminal patterns.

Existing initiatives offer practical reference points. For example, the World Economic Forum's Cybercrime Atlas seeks to build 'a shared knowledge base to disrupt cybercrime' through open-source research,[29] while joint operations coordinated through regional platforms such as Europol's European Cybercrime Centre,[30] which 'serves as the central hub for criminal information and intelligence', illustrate how shared intelligence can support coordinated investigations and enforcement actions.

To operationalize such approaches under the cybercrime convention, member states could consider establishing coordination mechanisms to synthesize inputs from national computer emergency response teams, law enforcement agencies and private sector entities. Automated mechanisms for sharing anonymized threat data, supported by standardized formats, may further enhance timeliness and scalability. In this context, data protection provisions within the convention play a significant role in providing safeguards for the handling and use of shared information, thereby reducing legal uncertainty associated with information exchange.

Aligning systems for operational readiness

Capacity extends beyond technical capabilities to include procedural interoperability. Technical capacity refers to the availability of tools, infrastructure and expertise required to conduct digital investigations, while procedural capacity refers to the legal and administrative frameworks that govern how and when such tools can be deployed. In the context of the cybercrime convention, capacity can be understood as the ability of national systems to communicate effectively, apply compatible evidentiary standards and respond within operationally relevant timeframes.

Cybercrime investigations are inherently time-sensitive. Certain forms of digital evidence, including IP logs, volatile memory and transaction data, may be altered, deleted or become inaccessible within short periods of time. As a result, delays in response can have a direct impact on the availability and reliability of evidence. Although the convention includes provisions encouraging the establishment of 24/7 points of contact to facilitate urgent cooperation, the existence of such mechanisms does not definitively ensure timely or effective responses. In practice, the capacity gap often arises from differences in legal procedures, administrative processes and institutional coordination.

In some jurisdictions, procedural requirements include judicial authorization, which can cause delays that do not align with the desired operational tempo of cybercrime investigations. In addition, disparities in technical expertise and resource availability across jurisdictions may further widen the capacity gap. While some states have developed specialized cybercrime units with advanced forensic capabilities, others continue to face constraints in accessing the necessary tools, training and institutional support. These differences can affect not only the quality of investigations, but also the ability to engage effectively in cross-border cooperation. In cross-border cases, these delays may be compounded when requests must be processed through multiple legal and administrative layers. Where one jurisdiction is able to process digital evidence rapidly and another is not, coordination becomes uneven, which can lead to delays in the broader investigative process.

The implications of such delays have been observed in cases involving financial cybercrime,[31] where funds may be transferred across multiple accounts and jurisdictions within short timeframes. In these contexts, delays in executing preservation or freezing requests may reduce the likelihood of asset recovery.

Similar challenges have been noted in efforts to address online child sexual exploitation,[32] where timely access to subscriber information and platform data is often critical to victim identification. Delays in obtaining such data may affect the speed and effectiveness of investigative responses.

Administrative differences further complicate cooperation. Variations in legal terminology, evidentiary thresholds and formatting requirements for mutual legal assistance requests can lead to delays or requests for clarification. In some cases, incomplete or non-standardized submissions may require revision and resubmission, extending investigation timelines.

The growing volume of digital evidence also presents practical challenges. Investigations increasingly involve large datasets, including logs, communications records and financial transactions, which require specialized tools and expertise to analyze. In some cases, forensic backlogs may delay the examination of evidence, further slowing investigative progress. Without sufficient investment in both technical infrastructure and human capital, these pressures may continue to strain existing systems and limit the effectiveness of enforcement efforts.

Addressing these challenges requires a focus on procedural interoperability. Member states may need to review their domestic frameworks to ensure that competent authorities are able to respond to urgent requests in a timely manner, consistent with the convention's provisions on expedited preservation and cooperation. The development of standardized templates and procedural guidelines may help reduce ambiguity in cross-border requests. Such templates could specify technical requirements for digital evidence, including cryptographic hash values, standardized time references and consistent metadata fields. Greater standardization may contribute to more efficient processing and reduce the likelihood of rejected or delayed requests.

In addition, capacity-building efforts may also benefit from a broader focus on institutional coordination. This could include strengthening collaboration between technical experts, investigators, prosecutors and judicial authorities. While such efforts might already exist in a regional context, such as the ASEAN Cybercrime Prosecutors' Roundtable Meetings,[33] there is a need to expand such efforts beyond regional collaboration, given the transnational nature of cybercrime. Without such coordination, the effectiveness of available technical capabilities may be constrained by procedural limitations.

Building trust through predictability and safeguards

International cooperation in cybercrime investigations often involves the exchange of sensitive data and the use of intrusive investigative measures. In such contexts, trust is both a prerequisite for cooperation and an outcome of sustained engagement. States may be cautious in sharing information due to concerns over data protection, potential misuse or the possibility of politically motivated requests. These concerns are shaped by differences in legal systems, governance structures and levels of institutional accountability. Trust cannot be established through legal provisions alone but is developed over time through consistent implementation, transparency and the demonstration of credible safeguards.

Trust is also influenced by perceptions of reciprocity and consistency in cooperation. States are more likely to engage in information sharing when they observe that their counterparts respond in a timely and proportionate manner to similar requests. Conversely, inconsistent or selective cooperation may undermine confidence and discourage future engagement. Over time, such dynamics can shape

informal expectations about which partnerships are reliable, potentially leading to uneven cooperation networks rather than truly global coordination.

Challenges relating to trust are reflected in broader debates on cross-border data access, as differing legal approaches to jurisdiction, privacy and law enforcement access can complicate cooperation.[34] Within the cybercrime convention, trust may be supported through provisions that emphasize safeguards, proportionality and data protection. When states request data under such frameworks, the responding state must have reasonable confidence that the requesting state will adhere to agreed standards regarding use limitation and data handling.

This underscores the importance of robust domestic legal frameworks, including judicial oversight mechanisms, accountability structures and enforceable data protection standards. States that demonstrate consistent adherence to such safeguards may be perceived as more reliable partners in cooperation.

One potential approach to strengthening trust is the use of voluntary implementation reporting. While not required under the cybercrime convention, similar practices in other domains, such as the Financial Action Task Force's mutual evaluation, illustrate how transparency can contribute to accountability and confidence building.[35] Under such an approach, states could publish periodic summaries outlining legislative developments, cooperation metrics, capacity-building efforts and oversight mechanisms. These reports would not require disclosure of sensitive operational details but could provide insight into how states are implementing their obligations. Over time, such practices may contribute to the development of shared expectations and norms, reducing uncertainty in cooperation and facilitating more consistent engagement.

Concerns regarding national sovereignty are often raised in discussions of international cooperation. However, the convention is structured as a state-led instrument that allows for implementation within domestic legal frameworks. Transparent and self-directed implementation may instead reinforce sovereignty by demonstrating that cooperation is grounded in national law while aligned with international commitments.

INCLUDING MULTI-STAKEHOLDERS IN IMPLEMENTATION

The importance of multi-stakeholder participation was summed up in Switzerland's contribution to the Ad Hoc Committee (AHC), which noted that '[m]eaningful participation of multi-stakeholders is essential to ensure an effective, inclusive, rights-respecting and transparent approach to combating cybercrime'.[36] Despite the difficulties and the continued lack of support for the convention from some non-governmental stakeholders and parts of the private sector, multiple stakeholders actively engaged and made useful contributions throughout the negotiations and the AHC process.

- The private sector outlined the impacts of elements of the convention (for example, how data requests work) and provided practical feedback and recommendations that were listened to and acted upon by many delegations.
- The human rights and digital rights community brought local expertise in terms of potential impacts on the ground, on real people, as well as experiences with other UN processes dealing with digital rights and cyber issues more broadly.
- Organizations dealing with victims of non-consensual sharing of images, online child sexual exploitation and connected criminal markets, such as human trafficking, contributed ground-level insights.
- Organizations focused on criminal market analysis highlighted developments in cybercrime and what is lacking in the international response, especially when it comes to existing instruments such as the UN Convention against Transnational Organized Crime (UNTOC), which has had a strong influence on the cybercrime convention.

Overall, the process demonstrated a remarkable ability among stakeholders to work across sectors and convey common positions on the most important issues, primarily on safeguards and human rights protections. Given how essential this convention is to confronting a range of societal threats, and the potential risks that still remain when it comes to the implementation of the safeguards, the input going forward will become even more meaningful.

Ensuring this type of open participation is the only way to ensure the proper interpretation of the convention, which is evident through the following articles, alongside the clear role of the treaty as an intergovernmental legal instrument. Compared to the UNTOC and the UN Convention against

Corruption (UNCAC), the cybercrime convention is notable for its broad range of references to the need for non-governmental participation. References to NGOs, the private sector and academia are mainstreamed throughout the convention, while limited references to these stakeholder groups appear in the UNTOC and the UNCAC. The private sector, in particular, is a vital partner when it comes to providing access to and sharing data, and civil society is referenced in connection with, among other things, victim protection, prevention, capacity building and technical assistance. These references emphasize that the convention's success will require the support and involvement of many different stakeholder groups.[37]

The benefits and value of non-government stakeholders, as recognized by the broad references in the convention, include the following:

- They help keep track of trends and developments in cybercrime. Governments and law enforcement do not have access to the latest global trends on their own, which is why organizations outside of the public sector exist – to give analysis based on a more diverse set of data, based on inputs from different sectors of society.
- They support capacity-building efforts. This is already happening, through initiatives and public–private partnerships that exist all over the world,[38] with diverse partners taking part in programmes. This type of trust building will help to unlock resources and connections, especially where it is needed in the Global South.
- They bring the voices of victims to the discussions. The perspectives of victims are integral to ensure that the convention is used to bring justice in these cases effectively.
- They keep a watchful eye on the safeguards, which are integral to the human rights compromise reached in this treaty.

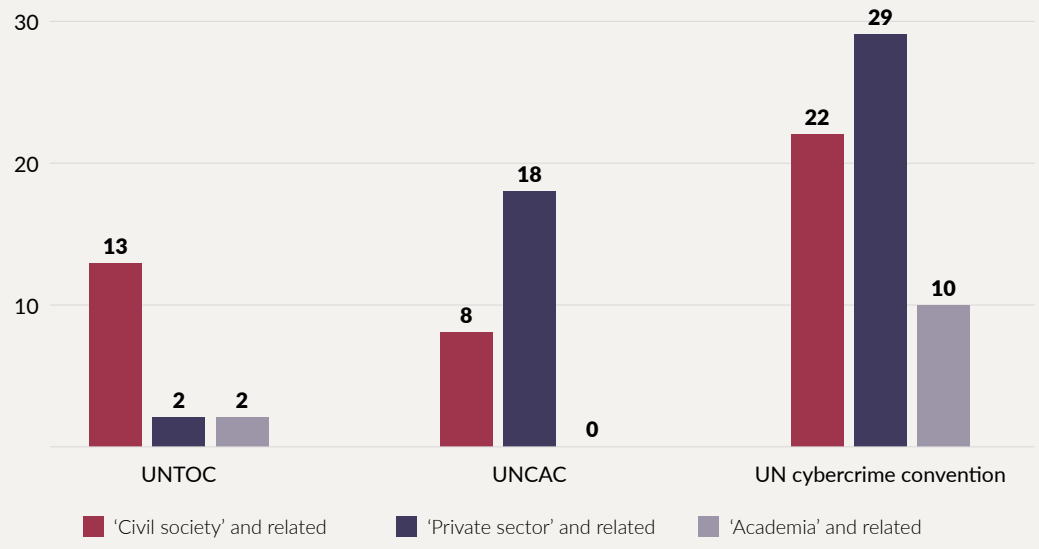


FIGURE 2 References to multi-stakeholders in the UN Convention against Cybercrime compared to the UNTOC and the UNCAC.

An event on the margins of the fourth session of the AHC emphasized the need for open participation to ensure the proper interpretation and implementation of the convention. *Photo: UNODC Civil Society Unit*

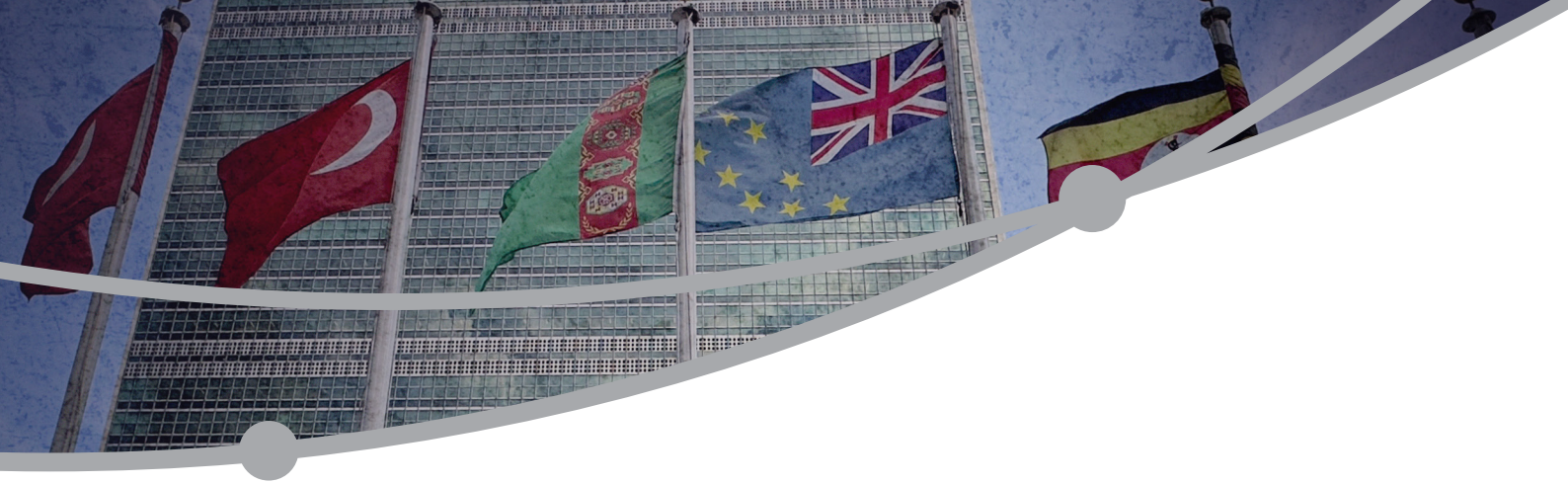
However, member states at the January 2026 meeting of the AHC failed to agree on the rules of procedure for its Conference of the Parties (CoP), including how it would engage with multi-stakeholders. As it stands, the CoP therefore has no basis on which to work.[39] This lack of consensus has delayed progress in implementing the convention, with the next AHC meeting scheduled to take place only in January 2027. In such a situation, the fight against cybercrime falters.[40] Furthermore, those invested in the convention's success should view the opposition from some parts of the private sector and the lack of widespread engagement since its adoption as warning signs.

At the same time, UN funding crises and the fragmentation of multilateralism further compound an uncertain future for the convention, including how resources will be leveraged to support its implementation. The adoption and wide approval of a new UN convention should be a boon for the UN Office on Drugs and Crime (UNODC), which acts as the convention's Secretariat. However, the convention's appearance on the scene coincides with a nadir in UN funding and political coherence. How current budget shortfalls to fund the convention's work will be met is unclear.[41]

The link that the cybercrime convention creates with existing treaties has been highlighted as an additional avenue for cooperation created by the moves towards an environmental crime protocol under the UNTOC.[42] For the UNODC, the convention is a welcome addition to its portfolio, alongside the UNTOC and the UNCAC, but creates risks if the resources and political will cannot be found to implement it effectively, or if the convention is used for malign purposes.

The model of the UNTOC and the UNCAC would provide the UNODC not only with secretariat services, but also with a clear, revenue-inviting capacity-building mandate. This would give the UNODC the authority to go into requesting countries to help them implement the convention under the UN flag. But given the current financial situation of the UN and the UNODC, it is difficult to envisage the activities coming to fruition to the same level as they did under the UNTOC and UNCAC regimes, in different political and financial times.

A major risk for the UNODC is that political disagreements and financial constraints consign the convention to stagnation. An even bigger risk is that the convention, perhaps following UNODC-led capacity building in authoritarian-minded countries, is used for malicious purposes – for example, making use of increased capacity provided by the UNODC to arrest dissidents, journalists or activists, under the guise of combating cybercrime.



CONCLUSION

The UN Convention against Cybercrime provides an important legal foundation for addressing cybercrime at the international level. Its adoption reflects a growing recognition of the need for more coordinated responses to an increasingly complex and transnational threat. However, its effectiveness will depend on how its provisions are translated into practice, and the extent to which diverse stakeholders are included in its implementation, providing their expertise and guarding against the treaty's misuse. Legal alignment alone is unlikely to produce meaningful outcomes without corresponding operational and institutional adjustments. The UNTOC provides clear lessons for avoiding such a scenario, including the lack of outcomes from its official review process and insufficient transparency and external engagement, resulting in limited evidence of its impact.[43] Addressing the knowledge gap through structured information sharing between countries and sectors, the capacity gap through procedural interoperability, and the trust gap through transparent and accountable mechanisms will be critical for the implementation of the cybercrime convention.

As cybercrime will continue to transform alongside technological developments, the implementation of the convention will need to remain adaptive, with ongoing refinement of practices and mechanisms, in contrast to the existing UNODC legal instruments, and how the AHC has addressed core issues since the convention's adoption. Its implementation should therefore be understood as an ongoing process rather than a one-time exercise – mechanisms will need to be continuously reviewed and adapted, as cyber threats develop and innovative technologies emerge. This includes not only refining legal and procedural frameworks, but also strengthening multi-stakeholder partnerships between governments, the private sector and other organizations that play a role in the broader cyber ecosystem.

Ultimately, the success of the cybercrime convention will be measured not only by the number of participating states, but by its ability to facilitate timely, effective, and coordinated responses to cybercrime through cross-regional and cross-sectoral cooperation. Under such conditions, it has the potential to serve as a practical foundation for international cooperation in the digital domain.

If member states cannot agree on a way forward on an inclusive, flexible and efficient set of modes of participation through its CoP, the convention may be doomed to fail. It needs open and trusting engagement with the private sector and civil society in order to succeed. The convention is no longer owned by those who proposed it, nor by those who initially rejected its existence. From its inception, it has been characterized by division, but moving forward it needs to belong to everyone who has a stake in it – member states across the political spectrum, alongside businesses and civil society groups that understand the vital part they have to play in putting it into practice, all working together under the auspices of the UN.

NOTES

1 Ian Tennant, UN cybercrime convention: A conference of contradictions in Hanoi, GI-TOC, 18 November 2025, https://globalinitiative.net/analysis/a-conference-of-contradictions-in-hanoi.

2 United Nations Convention against Cybercrime, Chapter XVIII: Penal matters, https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-16&chapter=18&clang=_en.

3 GI-TOC, Global Organized Crime Index 2025, https://ocindex.net.

4 The treaty largely deals with cyber-dependent crimes (offences that can *only* be carried out using a form of information and communications technology), but cooperation to address cyber-enabled crimes (offences carried out with the *support* of this technology) is also envisaged in the convention.

5 INTERPOL, Cybercrime, https://www.interpol.int/Crimes/Cybercrime.

6 GI-TOC, The ecosystem of organized crime, Intersections: Building blocks of a strategy against organized crime, July 2024, https://globalinitiative.net/wp-content/uploads/2024/07/ecosystem-of-organized-crime-global-initiative-gitoc-2024.pdf.

7 Summer Walker, Russian roulette: Cybercrime treaty risks a world of UN-sanctioned online control, GI-TOC, 22 July 2024, https://globalinitiative.net/analysis/cybercrime-treaty-risks-a-world-of-un-sanctioned-online-control.

8 GI-TOC, UN cyberwatch, https://globalinitiative.net/initiatives/un-cyberwatch.

9 Ibid.

10 Alexander Seger, Russian motivations behind the 'Hanoi Convention' against cybercrime, Just Security, 7 October 2025, https://www.justsecurity.org/122000/russian-motivations-hanoi-convention-cybercrime.

11 Ministry of Foreign Affairs of the Russian Federation, Press release on the adoption of the UN Convention against Cybercrime, 24 December 2024, https://mid.ru/en/foreign_policy/news/1989289; Permanent Mission of the Russian Federation to the International Organizations in Vienna, Supplementary protocol to the 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, Draft supplementary protocol, UNODC, 22 May 2026, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Protocol/1st_session/Russian_Federation_ENG_24_June_2026.pdf.

12 Ibid.

13 UNODC, Hanoi convention: Canada's statement, 31 October 2025, https://hanoiconvention.org/statement/canadas-statement.

14 Letter from the Software and Information Industry Association and the Computer and Communications Industry Association to US Secretary of State Antony Blinken, Attorney General Merrick Garland, Secretary of Commerce Gina Raimondo and Assistant to the President Jake Sullivan on the subject of the UN Convention against Cybercrime, 1 November 2024, https://www.siia.net/wp-content/uploads/2024/11/Industry-Letter-UN-Convention-Against-Cybercrime.pdf.

15 Council of Europe, Fighting cybercrime: EU to sign UN Convention on cybercrime, Press release, 13 October 2025, https://www.consilium.europa.eu/en/press/press-releases/2025/10/13/fighting-cybercrime-eu-to-sign-un-convention-on-cybercrime.

16 UNODC, Hanoi convention: Federative Republic of Brazil's statement, 25 October 2025, https://hanoiconvention.org/statement/federative-republic-of-brazils-statement.

17 Simon Sharwood, Cisco calls for United Nations to revisit cyber-crime convention, The Register, 22 August 2024, https://www.theregister.com/2024/08/22/cisco_criticizes_un_cybercrime_convention.

18 Francesco Guarascio, UN cybercrime pact to be signed in Hanoi raises hopes, concerns, Reuters, 22 October 2025, https://www.reuters.com/sustainability/society-equity/un-cybercrime-pact-be-signed-hanoi-raises-hopes-concerns-2025-10-22.

19 Human Rights Watch, Joint statement on the signing of the UN Convention on Cybercrime, 24 October 2025, https://www.hrw.org/news/2025/10/24/joint-statement-on-the-signing-of-the-un-convention-on-cybercrime.

20 David Wright, A global framework for change: Discussing NCII at the UN Cybercrime Convention, SWGfL, 10 October 2024, https://swgfl.org.uk/magazine/a-global-framework-for-change-discussing-ncii-at-the-un-cybercrime-convention.

21 Kristina Amerhauser and Alex Goodwin, A world of deceit: Mapping the landscape of the global scam centre phenomenon, GI-TOC, March 2026, https://globalinitiative.net/analysis/mapping-global-scam-center-phenomenon.

22 INTERPOL, INTERPOL welcomes adoption of UN convention against cybercrime, 23 December 2024, https://www.interpol.int/en/News-and-Events/News/2024/INTERPOL-welcomes-adoption-of-UN-convention-against-cybercrime.

23 Mark Shaw et al, Is the UNTOC working? An assessment of the implementation and impact of the Palermo Convention, GI-TOC, October 2024, https://globalinitiative.net/analysis/is-the-untoc-working.

24 Andreas Wolter, Security: The Need-to-know principle, Microsoft Tech Community, 3 February 2021, https://techcommunity.microsoft.com/blog/azuresqlblog/security-the-need-to-know-principle/2112393.

25 Nilantha Prasad et al, A survey of cyber threat attribution: Challenges, techniques, and future directions, *Computers & Security*, 157 (October 2025), 104606, https://www.sciencedirect.com/science/article/pii/S0167404825002950.

26 WEF suggests multi stakeholder approach to tackle ransomware, Industrial Cyber, 26 May 2021, https://industrialcyber.co/news/wef-suggests-multi-stakeholder-approach-to-tackle-ransomware.

27 GI-TOC, The rise and fall of the Conti ransomware group, Deep Dive podcast: Episode 32, https://globalinitiative.net/analysis/conti-ransomware-group-cybercrime.

28 GI-TOC, Compound crime: Cyber scam operations in Southeast Asia, May 2025, https://globalinitiative.net/analysis/compound-crime-cyber-scam-operations-in-southeast-asia; Kristina Amerhauser and Audrey Till, The business of exploitation: The economics of cyber scam operations in Southeast Asia, GI-TOC, August 2025, https://globalinitiative.net/analysis/cyber-scam-operations-southeast-asia.

29 World Economic Forum, Cybercrime Atlas, https://initiatives.weforum.org/cybercrime-atlas/home.

30 Europol, European Cybercrime Centre – EC3, https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3.

31 Best Cyber Crime Lawyer, Money recovery delay in cyber crime case, https://bestcybercrimelawyer.in/2026/02/25/money-recovery-delay-in-cyber-crime-case.

32 Financial Action Task Force, Detecting, disrupting and investigating online child sexual exploitation: Using financial intelligence to protect children from harm, 2025, https://www.fatf-gafi.org/en/publications/Fatfgeneral/Online-child-sexual-exploitation.html.

33 Singapore International Cyber Week, ASEAN Cybercrime Prosecutors' Roundtable Meeting, 22 October 2025, https://www.sicw.gov.sg/events/22-oct/asean-cybercrime-prosecutors-roundtable-meeting-acprm.

34 For instance, legal disputes and policy developments, including those associated with the *Microsoft Corp. v. United States* case and subsequent legislative responses such as the US CLOUD Act. 'The [Microsoft] case centered on a uniquely-different warrant that was issued by US prosecutors in that it was for data stored in an email account stored by Microsoft overseas. Prosecutors said that because the data was hosted by a US-based company, Microsoft must comply. But the judges concluded that Congress did not intend the law used in the case – the Stored Communications Act – to apply outside the US'; Zack Whittaker, In privacy victory, Microsoft wins appeal over foreign data warrant, ZDNET, 14 July 2016, https://www.zdnet.com/article/microsoft-wins-appeal-over-warrant-for-overseas-emails. See also: Felicity Fisher, Victory for digital privacy in Microsoft warrant case: US court confirms that US data warrants do not apply overseas, Field Fisher, 18 July 2016, https://www.fieldfisher.com/en/services/privacy-security-and-information/privacy-security-and-information-law-blog/victory-for-digital-privacy-in-microsoft-warrant-case-us-court-confirms-that-us-data-warrants-do-not-apply-overseas; US Congress, CLOUD Act, https://www.congress.gov/bill/115th-congress/house-bill/4943.

35 Financial Action Task Force, Mutual evaluations, https://www.fatf-gafi.org/en/topics/mutual-evaluations.html.

36 UNODC, Switzerland's submission relating to the preparation of the draft text of the rules of procedure of the Conference of the States Parties to the United Nations Convention against Cybercrime, 6 June 2025, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/RoP_session/Comments_by_MS_06062025/Switzerland_ROP_of_the_UN_Convention_against_Cybercrime_6_June_2025.pdf.

37 This is reiterated in the Preamble, Article 34 (assistance to victims), Article 53 (prevention), Article 54 (capacity building), Article 55 (exchange of information), Article 56 (technical assistance and development) and Article 57 (Conference of States parties).

38 UNODC, Public–private partnerships on cybercrime: Regional perspectives on best practices, challenges, and opportunities from the Americas, Africa, and Asia, 2024,

https://www.unodc.org/documents/NGO/PDF/CSU-CyberCrime-240807-WEB.pdf.

39 Ian Tennant, Deadlock for UN cybercrime treaty: Familiar issues derail discussions in Vienna, GI-TOC, 10 February 2026, https://globalinitiative.net/analysis/deadlock-united-nations-cybercrime-treaty.

40 Ibid.

41 Ian Tennant, Ongoing uncertainty and an unrelenting agenda: The UNODC in 2026, GI-TOC, 23 January 2026, https://globalinitiative.net/analysis/ongoing-uncertainty-and-an-unrelenting-agenda-the-unodc-in-2026.

42 John Scanlon, Momentum is building for a protocol on crimes that affect the environment, Illuminem, 28 October 2025, https://illuminem.com/illuminemvoices/momentum-is-building-for-a-protocol-on-crimes-that-ffect-the-environment; Ian Tennant, Simone Haysom and Tiphaine Chapeau, A new protocol for the UNTOC?, A guidance note for the 1st meeting of the new Intergovernmental Expert Group on crimes that affect the environment, GI-TOC, June 2025, https://globalinitiative.net/analysis/new-protocol-untoc-crimes-that-affect-the-environment; Ian Tennant, When 'why?' becomes 'why not?' The case for a new global framework to tackle environmental crime, GI-TOC, 16 April 2026, https://globalinitiative.net/analysis/the-case-for-a-new-global-framework-to-tackle-environmental-crime.

43 Mark Shaw et al, Is the UNTOC working? An assessment of the implementation and impact of the Palermo Convention, GI-TOC, October 2024, https://globalinitiative.net/analysis/is-the-untoc-working.

GLOBAL INITIATIVE
AGAINST TRANSNATIONAL ORGANIZED CRIME

ABOUT THE GLOBAL INITIATIVE

The Global Initiative Against Transnational Organized Crime is a global network with 800 Network Experts around the world. The Global Initiative provides a platform to promote greater debate and innovative approaches as the building blocks to an inclusive global strategy against organized crime.

www.globalinitiative.net