JURIS NEXUS: JOURNAL OF LAW & MULTIDISCIPLINARY STUDIES
(An Online Referred Peer-Reviewed Journal)
ISSN: XXXX-XXXX I PIF: X.XX I VOL. 01 I Mar. I 2026
Website – www.JNJLMS.com Emai Id - contact@JNJLMS.com

# ROLE OF INTERNATIONAL ORGANISATIONS IN PREVENTING CYBER CRIME: A GLOBAL GOVERNANCE PERSPECTIVE

**Prof. (Dr.) V.P. Rai**
Dept. of Law, B.S.A. College, DBRAU, Agra
**Nivedita Singh**
Assistant Professor, L.B.S. Law College, Tiwariganj, Lucknow

**ABSTRACT**

*The rapid expansion of digital technologies has transformed global communication, commerce, and governance while simultaneously facilitating the emergence of cybercrime as a serious transnational threat. Cyber offences such as data breaches, ransom ware attacks, online fraud, and cyber terrorism transcend territorial boundaries and challenge the effectiveness of state-centric legal frameworks. Given the borderless nature of cyberspace, unilateral national responses are often inadequate to address cybercrime effectively. This paper examines the role of international organizations in preventing cybercrime from a global governance perspective. It analyses how institutions such as the United Nations, INTERPOL, the International Telecommunication Union, and regional organizations contribute to norm-setting, legal harmonization, operational cooperation, and capacity building. Adopting a doctrinal and analytical methodology, the study argues that although international cyber governance remains fragmented and largely dependent on soft law, international organizations play an indispensable role in fostering cooperation and bridging legal and technological disparities among states. The paper concludes that strengthening institutional coordination and adaptive governance mechanisms is essential to ensuring a secure and resilient global cyberspace.*

**KEYWODRS:** *Cyber Crime, International Organizations, Global Governance, Cyber Security, International Cooperation and etc.*

## INTRODUCTION

The rapid advancement of digital technologies has fundamentally reshaped contemporary societies by enabling unprecedented levels of connectivity, efficiency, and innovation. Information and communication technologies now underpin critical sectors such as banking,

healthcare, governance, and global commerce, making cyberspace an indispensable domain of modern life[1]. However, this accelerated digitalization has also created new vulnerabilities that are increasingly exploited by malicious actors. Cyber-crime has emerged as one of the most significant unintended consequences of technological progress, leveraging the speed, anonymity, and global reach of digital networks[2]. Unlike traditional crimes that are territorially confined, cyber offences are inherently transnational, allowing perpetrators to operate across jurisdictions while targeting victims in multiple states simultaneously[3]. This borderless character complicates detection, attribution, and enforcement, placing significant strain on domestic legal systems. As digital dependence deepens, cybercrime has evolved from isolated incidents into organized and sophisticated activities that threaten economic stability, national security, and individual privacy.

**Nature and Scope of Cyber Crimes**

Cybercrimes encompass a diverse range of unlawful activities committed through or against digital systems and networks. These offences include data breaches involving unauthorized access to sensitive information, ransom ware attacks that disrupt essential services, online fraud schemes exploiting financial systems, and cyber terrorism targeting critical infrastructure[4]. The scope of cyber-crime continues to expand with the use of emerging technologies such as artificial intelligence, crypto currencies, and anonymization tools, which enable criminals to evade detection and obscure accountability. Importantly, the harm caused by cybercrime extends beyond financial loss, undermining trust in digital governance and exacerbating inequalities between technologically advanced and developing states.

**Problem Statement and Research Gap**

Despite the growing recognition of cybercrime as a global threat, existing responses remain fragmented and uneven. While many states have enacted domestic cyber laws, significant disparities persist in legal definitions, enforcement capacity, and procedural standards. These inconsistencies create jurisdictional loopholes that cyber criminals exploit[5]. Although international organizations have assumed a greater role in addressing cybercrime through norm-setting and cooperation, scholarly analysis often remains descriptive or institution-specific. There is a lack of integrated examination of how international organisations collectively function as governance actors in cybercrime prevention.

[1] Manuel Castells, *The Rise of the Network Society* 69–71 (2d ed. 2010).
[2] Susan W. Brenner, *Cybercrime: Criminal Threats from Cyberspace* 12–15 (2010).
[3] David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 Stan. L. Rev. 1367, 1370–72 (1996).
[4] Council of Europe, Explanatory Report to the Convention on Cybercrime, 38–41 (2001).
[5] Michael N. Schmitt, *Peacetime Cyber Responses and Wartime Cyber Operations*, 55 Int'l L. Stud. 89, 96–98 (2018).

### Objectives of the Study

The primary objective of this study is to critically examine the role of international organizations in preventing cybercrime. The study aims to analyze their contribution to legal harmonization, operational cooperation, and capacity building, assess the challenges faced by these institutions, and propose measures to strengthen global cyber governance frameworks.

### Research Methodology and Structure of the Paper

This paper adopts a doctrinal and analytical research methodology based on secondary sources, including international legal instruments, policy documents, and scholarly literature.

## Conceptual and Theoretical Framework

### 1. Concept and Classification of Cyber Crime

Cyber-crime, as a legal and socio-technical concept, refers to unlawful activities in which computers, digital networks, or information systems function either as the primary targets or as essential instruments of the offence[6]. Unlike conventional crimes, cyber-crimes are embedded within complex technological environments, making their identification, categorisation, and regulation particularly challenging[7]. The absence of a universally accepted definition reflects the evolving nature of cyber threats and the diversity of legal approaches adopted by states. Broadly, cyber-crimes may be classified into several categories based on their nature and impact. These include crimes against individuals, such as identity theft, cyber stalking, and online fraud, crimes against property, including data theft, intellectual property infringement, and ransomware attacks, and crimes against states or public order, such as cyber espionage, cyber terrorism, and attacks on critical infrastructure. Another important classification distinguishes between cyber-dependent crimes, which can only be committed using digital technologies, and cyber-enabled crimes, where traditional offences are facilitated by digital means.

### 2. Transnational Nature of Cyber Offences

One of the defining characteristics of cybercrime is its inherently transnational nature, which distinguishes it from most traditional criminal activities. Cyber offences frequently involve multiple jurisdictions simultaneously, as the infrastructure used to commit the offence, the location of the perpetrator, the servers hosting data, and the place where harm occurs may all fall within different states[8]. The anonymity afforded by digital technologies further exacerbates these

[6] Susan W. Brenner, *Cybercrime: Criminal Threats from Cyberspace* 7–9 (2010)
[7] U.N. Office on Drugs & Crime, Comprehensive Study on Cybercrime, at 17–19 (2013).
[8] David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 Stan. L. Rev. 1367, 1370–72 (1996).

challenges, allowing offenders to conceal their identities and exploit jurisdictional inconsistencies. Transnational cybercrime networks often operate through decentralized structures, leveraging global connectivity to coordinate illicit activities across borders with minimal physical presence. As a result, cybercrime has become a shared global concern rather than a purely domestic law enforcement issue. The transnational dimension also raises complex questions relating to sovereignty, jurisdiction, and state responsibility, particularly when cyber activities originate from or pass through multiple national territories.

### 3. Global Governance and Cyberspace

The concept of global governance provides a useful theoretical framework for analyzing international responses to cybercrime. Global governance refers to the collective management of transnational issues through formal and informal institutions, norms, and processes involving states, international organizations, and non-state actors[9]. Cyberspace, by its very nature, resists exclusive state control, as digital networks transcend territorial boundaries and involve multiple stakeholders, including private corporations and civil society. Traditional state-centric models of governance are therefore inadequate for addressing the complex regulatory challenges posed by cybercrime. Global governance theory emphasizes cooperation, coordination, and shared responsibility, making it particularly relevant to cyberspace regulation. International organizations function as central nodes within this governance architecture by facilitating norm-setting, coordinating policy responses, and providing platforms for dialogue and capacity building[10]. They help reconcile competing national interests while promoting collective security and stability in the digital domain. From a governance perspective, cybercrime prevention is not merely a matter of law enforcement but involves broader considerations of trust, accountability, and institutional legitimacy.

### 4. Need for International Cooperation

International cooperation is widely regarded as an indispensable component of effective cybercrime prevention. Given the transnational and technologically sophisticated nature of cyber offences, no single state possesses the capacity or jurisdictional reach to address these challenges independently. Cooperative mechanisms enable states to share intelligence, harmonies legal standards, and coordinate enforcement actions across borders. International cooperation also plays a crucial role in capacity building, particularly for developing states that may lack the technical expertise or resources required to combat cybercrime effectively. Through joint initiatives, training programmers, and technical assistance, international institutions contribute to reducing disparities in cyber security preparedness. Moreover, cooperation fosters trust among

[9] James N. Rosenau, *Governance in the Twenty-First Century*, 1 Global Governance 13, 15–17 (1995).
[10] U.N.G.A. Res. 75/240, 6–9 (Dec. 31, 2020).

states, which is essential for timely information exchange and collaborative responses to cyber incidents. However, achieving meaningful cooperation is often hindered by political tensions, concerns over sovereignty, and divergent national priorities. Issues such as data protection, surveillance, and attribution further complicate collaborative efforts. Despite these challenges, international cooperation remains the most viable strategy for addressing cybercrime in a globally interconnected environment. It provides a framework for collective action that balances national interests with shared security objectives.

## International Legal and Institutional Framework for Cyber Crime Prevention

### 1. Evolution of International Cyber Law

The evolution of international cyber law has been shaped by the growing recognition that cyberspace constitutes a shared global domain requiring collective regulation[11]. In its early stages, international law did not specifically address cyber activities, as technological developments outpaced normative responses. Traditional principles of international law, such as sovereignty, non-intervention, and jurisdiction were initially applied by analogy to cyber conduct, often resulting in ambiguity and interpretative challenges. As cyber incidents increased in frequency and severity, states and international institutions began acknowledging the limitations of purely domestic legal frameworks in addressing transnational cybercrimes. This led to the gradual emergence of international cyber law through a combination of treaties, resolutions, guidelines, and state practice. Instruments such as multilateral conventions, regional agreements, and United Nations resolutions have contributed to shaping normative expectations regarding state responsibility and cooperation in cyberspace. The development of cyber law has largely followed a fragmented trajectory, relying heavily on soft law mechanisms due to the lack of consensus among states on binding obligations[12].

### 2. Harmonization of Cyber Laws and Jurisdictional Challenges

One of the most pressing challenges in combating cybercrime at the international level lies in the lack of harmonization among national cyber laws. States differ significantly in how they define cyber offences, prescribe penalties, regulate digital evidence, and assert jurisdiction over cyber activities. These disparities create enforcement gaps that cyber criminals exploit by operating across jurisdictions with weak or inconsistent legal standards[13]. Jurisdictional challenges are further compounded by the borderless nature of cyberspace, where the location of the perpetrator, victim, data servers, and harmful effects may all fall within different territorial

[11] Joseph S. Nye, Jr., *The Regime Complex for Managing Global Cyber Activities*, 1–3 (2014).
[12] Martha Finne more & Duncan B. Hollis, *Constructing Norms for Global Cyber security*, 110 Am. J. Int'l L. 425, 440–42 (2016).
[13] Susan W. Brenner, *Cybercrime Jurisdiction*, 46 Crime, L. & Soc. Change 189, 194–96 (2006).

boundaries. Traditional jurisdictional principles based on territoriality and nationality often prove inadequate in addressing such complex scenarios. Despite these challenges, international cooperation mechanisms, including mutual legal assistance treaties and cross-border investigative frameworks, represent important steps toward mitigating jurisdictional obstacles. The effectiveness of these mechanisms, however, depends largely on political will, institutional capacity, and sustained international engagement.

### 3. Role of International Norms and Policy Instruments

In the absence of comprehensive binding treaties, international norms and policy instruments have assumed a central role in shaping state behaviour in cyberspace. These norms, often articulated through resolutions, declarations, and expert group reports, provide guidance on acceptable conduct and cooperative practices in preventing cybercrime[14]. International organizations have been instrumental in developing such norms by facilitating dialogue, building consensus, and promoting shared understandings of cyber threats. Normative frameworks encourage states to adopt measures such as information sharing, capacity building, and respect for international law in cyberspace. While non-binding in nature, these instruments carry significant persuasive value and contribute to the gradual formation of customary international law. Policy instruments also serve as platforms for confidence-building measures, helping to reduce mistrust and misperceptions among states regarding cyber activities[15].

## Role of International Organizations in Preventing Cyber Crime

- **United Nations**

The United Nations has emerged as a central platform for addressing cybercrime and promoting responsible state behaviour in cyberspace through its normative and diplomatic initiatives[16]. While the UN does not function as an enforcement agency, its contribution lies in shaping international consensus on the application of existing international law to cyber activities. Through forums such as the General Assembly and specialized processes, the UN has facilitated sustained dialogue among states on cyber security challenges, thereby reducing fragmentation in policy approaches. UN-led initiatives emphasize the importance of state responsibility, due diligence, and cooperation in preventing malicious cyber activities emanating from national territories. By encouraging transparency and confidence-building measures, the United Nations seeks to mitigate the risk of cyber conflicts and escalation. The organization has also highlighted the need to protect critical infrastructure and uphold human rights in the digital domain,

[14] U.N. Group of Governmental Experts, Report on Developments in the Field of Information and Telecommunications, 13–16 (2015).
[15] U.N. Secretary-General, Roadmap for Digital Cooperation, at 17–18 (2020).
[16] U.N. G.A. Res. 75/240

recognizing that cybercrime can have far-reaching social and economic consequences[17]. Importantly, the UN provides a neutral forum where states with divergent political and strategic interests can engage constructively on cyber governance issues.

**INTERPOL**

INTERPOL plays a pivotal operational role in preventing cybercrime by facilitating cross-border cooperation among national law enforcement agencies[18]. Given that cyber offences frequently involve multiple jurisdictions, effective investigation and prosecution depend on timely information exchange and coordinated action. INTERPOL provides a secure communication platform that enables member states to share intelligence, issue alerts, and coordinate responses to cyber incidents[19]. Through specialized cybercrime units and task forces, INTERPOL supports joint investigations targeting organized cyber-criminal networks engaged in activities such as ransom ware attacks, online fraud, and digital extortion. The organization also assists in capacity building by offering training programmers, technical tools, and best practice guidelines to law enforcement agencies, particularly in developing countries. By strengthening investigative capabilities and fostering trust among national authorities, INTERPOL helps bridge enforcement gaps that cyber criminals routinely exploit.

1. **International Telecommunication Union**

The International Telecommunication Union (ITU) contributes to cybercrime prevention primarily through its role in developing technical standards, promoting cyber security capacity building, and fostering international cooperation in the telecommunications sector[20]. As a specialized agency of the United Nations, the ITU focuses on ensuring the secure and resilient functioning of global communication networks[21]. Its initiatives address the technical dimensions of cyber threats by encouraging the adoption of best practices, risk management frameworks, and security standards across member states. The ITU also plays a significant role in assisting states, particularly developing and least developed countries, in enhancing their national cyber security preparedness.

[17] U.N. Human Rights Council, The Right to Privacy in the Digital Age, 20–23 (2018).
[18] INTERPOL, Global Cybercrime Strategy, at 5–7 (2022).
[19] INTERPOL, Cybercrime Knowledge Exchange, at 3–4 (2021).
[20] Int'l Telecomm. Union, Global Cyber security Agenda, at 3–5 (2007).
[21] Constitution and Convention of the International Telecommunication Union arts. 1–4, Dec. 22, 1992.

JURIS NEXUS: JOURNAL OF LAW & MULTIDISCIPLINARY STUDIES
(An Online Referred Peer-Reviewed Journal)
ISSN: XXXX-XXXX I PIF: X.XX I VOL. 01 I Mar. I 2026
Website – www.JNJLMS.com Emai Id - contact@JNJLMS.com

### 2. Regional Organisations

Regional organizations play an increasingly important role in addressing cybercrime by tailoring cooperative mechanisms to regional contexts and shared legal traditions[22]. These organizations often act as intermediaries between global norms and national implementation, facilitating closer coordination among neighboring states. Regional frameworks enable member states to develop common legal standards, share best practices, and conduct joint capacity-building initiatives. Due to geographical proximity and shared security concerns, regional cooperation can often be more agile and responsive than global mechanisms. Regional organizations also provide platforms for trust-building and dialogue, which are essential for effective information sharing and coordinated responses to cyber incidents. However, regional approaches may suffer from uneven participation and varying levels of commitment among member states. Differences in economic development, technical capacity, and political priorities can limit the effectiveness of regional initiatives. Additionally, regional frameworks may lack the global reach required to address cybercrimes that extend beyond regional boundaries. Despite these challenges, regional organisations complement international efforts by reinforcing cooperation at an intermediate level and enhancing the practical implementation of cyber governance norms. Their role demonstrates that cyber-crime prevention requires multi-layered governance structures operating at global, regional, and national levels.

### 3. Comparative Assessment

A comparative assessment of international organisational mechanisms reveals both complementarities and limitations in global cyber-crime prevention efforts. While institutions such as the United Nations focus on norm-setting and policy coordination, organisations like INTERPOL provide operational support, and bodies such as the ITU address technical and capacity-related aspects[23]. This functional differentiation allows international organisations to address cyber crime from multiple angles, reflecting the complexity of the threat landscape[24]. However, the absence of a central coordinating authority often leads to overlap, fragmentation, and inconsistent implementation. Institutional effectiveness is further constrained by voluntary compliance, limited enforcement powers, and geopolitical rivalries among states. Despite these shortcomings, international organisations collectively contribute to reducing regulatory gaps, enhancing cooperation, and promoting shared responsibility. Their role is particularly significant in facilitating dialogue, building trust, and supporting states with limited resources. A coordinated and synergistic approach among international organisations is essential for

[22] Martha Finne more & Duncan B. Hollis, *Constructing Norms for Global Cyber security*, 11:00 Am. J. Int'l L. 425, 434–36 (2016).
[23] INTERPOL, Global Cybercrime Strategy, at 6–8 (2022).
[24] Europol, Internet Organized Crime Threat Assessment, at 10–12 (2023).

maximising their impact. Strengthening institutional cooperation and clarifying mandates could enhance the effectiveness of global cyber crime prevention strategies. This comparative analysis underscores that while international organisations cannot eliminate cyber crime, they remain indispensable actors in shaping a cooperative and resilient global cyberspace.

## Challenges, Limitations, and Emerging Issues

### 1. Legal and Technological Disparities among States

One of the most significant challenges in preventing cyber crime at the international level arises from deep legal and technological disparities among states. Countries vary widely in their levels of digital infrastructure, cyber security preparedness, and legislative development. While some states possess comprehensive cyber laws, specialised enforcement agencies, and advanced forensic capabilities, others continue to rely on outdated legal frameworks ill-suited to address modern cyber threats. These disparities create asymmetries in enforcement capacity, allowing cyber criminals to exploit jurisdictions with weaker regulatory and technological safeguards[25]. Differences in legal definitions of cyber offences, evidentiary standards, and procedural rules further complicate international cooperation. In many cases, conduct considered criminal in one jurisdiction may not be explicitly prohibited in another, hindering extradition and mutual legal assistance. Technological disparities also affect states' ability to detect, investigate, and respond to cyber incidents in a timely manner. Developing countries, in particular, often face resource constraints that limit investment in cyber security infrastructure and skilled personnel. As a result, they may become safe havens or transit points for cyber criminal activities. These inequalities undermine collective efforts to create a secure global cyberspace and highlight the need for targeted capacity-building initiatives. Addressing legal and technological disparities is therefore essential for ensuring that international cyber crime prevention frameworks operate effectively and equitably across different regions.

### 2. Political, Sovereignty, and Enforcement Constraints

Political considerations and concerns over state sovereignty present substantial obstacles to effective international cooperation in cyber crime prevention[26]. States remain cautious about sharing sensitive information related to cyber incidents, intelligence capabilities, and critical infrastructure vulnerabilities due to fears of national security breaches and loss of strategic advantage. Sovereignty concerns are particularly pronounced in cyberspace, where actions such as cross-border investigations, data access requests, and attribution of cyber attacks may be perceived as intrusive or illegitimate. These sensitivities often result in limited transparency and

[25] Susan W. Brenner, *Cybercrime Jurisdiction*, 46 Crime, L. & Soc. Change 189, 194–96 (2006).
[26] Michael N. Schmitt, *Peacetime Cyber Responses*, 55 Int'l L. Stud. 89, 96–98 (2018).

reluctance to cooperate fully with international mechanisms. Enforcement constraints further exacerbate these challenges, as international organisations generally lack coercive powers and depend on voluntary compliance by member states. These constraints highlight the limitations of existing international frameworks and underscore the need for confidence-building measures that balance sovereignty with shared security interests.

### 3. Capacity-Building Gaps and Resource Constraints

Capacity-building remains a critical yet uneven component of international cyber crime prevention efforts. While international organizations have initiated numerous training programmers and technical assistance projects, the scale and sustainability of these initiatives often fall short of actual needs. Many states lack adequately trained personnel, specialized cyber crime units, and access to advanced investigative tools. Resource constraints are particularly acute in developing and least developed countries, where competing socio-economic priorities limit investment in cyber security. The absence of sustained funding and institutional support undermines the long-term effectiveness of capacity-building efforts. Moreover, capacity-building initiatives sometimes fail to account for local legal, cultural, and institutional contexts, reducing their practical applicability. The rapid evolution of cyber technologies further complicates capacity development, as skills and tools can quickly become obsolete. International organizations play a crucial role in addressing these gaps, but their efforts must be supported by sustained political commitment and resource allocation from member states.

### 4. Emerging Cyber Threats and Adaptive Criminal Techniques

The dynamic nature of cyber crime presents ongoing challenges to international prevention efforts, as criminal techniques continuously evolve in response to technological advancements and regulatory measures[27]. Emerging threats such as artificial intelligence-driven attacks, deep fake technology, and the misuse of crypto currencies have expanded the cyber crime landscape. These technologies enable criminals to automate attacks, evade detection, and obscure financial transactions, complicating investigation and enforcement[28]. The growing reliance on digital platforms and remote systems has also increased exposure to cyber risks, particularly in critical sectors such as healthcare, finance, and energy[29]. International frameworks often struggle to adapt quickly to these developments, as norm-setting and legal reform processes tend to be slow and consensus-driven. This lag creates regulatory gaps that cyber criminals exploit. Additionally, the increasing involvement of non-state actors and organised criminal networks adds complexity to attribution and accountability.

[27] U.N.O.D.C., Cybercrime and Emerging Technologies, at 6–8 (2022).
[28] Financial Action Task Force, Virtual Assets Red Flag Indicators, at 4–6 (2021).
[29] World Economic Forum, Global Cyber security Outlook, at 12–14 (2023).

JURIS NEXUS: JOURNAL OF LAW & MULTIDISCIPLINARY STUDIES
(An Online Referred Peer-Reviewed Journal)
ISSN: XXXX-XXXX I PIF: X.XX I VOL. 01 I Mar. I 2026
Website – www.JNJLMS.com Emai Id - contact@JNJLMS.com

## Conclusion

In light of the findings, the study underscores the need to strengthen global cyber governance through more coherent, inclusive, and adaptive frameworks. One key recommendation is the enhancement of coordination among international organizations to reduce institutional fragmentation and overlap. Clearer delineation of roles and improved information-sharing mechanisms could significantly enhance the effectiveness of collective responses to cyber crime. The study also highlights the importance of advancing legal harmonization by encouraging states to adopt common definitions of cyber offences and standardized procedural rules. While complete uniformity may be unrealistic, incremental convergence can help close jurisdictional loopholes exploited by cyber criminals. Capacity-building should be prioritized as a long-term investment rather than treated as a supplementary measure. International organizations, in partnership with technologically advanced states and private stakeholders, should expand technical assistance programmers tailored to the specific needs of developing countries.

While this study provides a comprehensive analysis of the role of international organizations in preventing cyber crime, it also opens several avenues for future research. Further empirical studies could assess the practical effectiveness of specific international initiatives and capacity-building programmers, offering data-driven insights into what works and what requires reform. Comparative research examining regional cyber governance models could deepen understanding of how regional organizations complement global frameworks. Future scholarship may also explore the intersection between cyber crime and emerging technologies such as artificial intelligence, quantum computing, and digital currencies, which are likely to reshape both criminal methods and regulatory responses. Another important area for research lies in examining accountability mechanisms for state and non-state actors involved in cyber activities, particularly in the context of attribution and enforcement. Interdisciplinary approaches integrating law, technology, and international relations would be particularly valuable in addressing the multifaceted nature of cyber crime. As cyberspace continues to evolve, academic research must remain adaptive and forward-looking. By identifying these future directions, the study emphasizes that cyber crime prevention is an ongoing process requiring continuous scholarly engagement and institutional innovation. Strengthening the role of international organizations will remain central to ensuring a secure, resilient, and trustworthy global cyberspace.