Commission on Crime Prevention and Criminal Justice

Agenda: Facilitating an action plan towards the integration of Digital Technologies into Criminal Justice Systems in addressing cybercrime.

LETTER FROM THE EXECUTIVE BOARD

Greetings delegates,

It is an honour to be serving as the executive board at the Commission on Crime Prevention and Criminal Justice at SJBHSMUN 2025. The committee you will be a part of, will be discussing the crucial topic of *'Facilitating an action plan towards the integration of Digital Technologies into Criminal Justice Systems in addressing cybercrime.'* You will be gathering for a formal meet during a span of three days, representing different countries and hopefully, coming to a conclusion.

To help you with your research, we have prepared this background guide for you so that you are familiar with the agenda. Please note this guide, as the name suggests is to merely provide you with a basic idea regarding the agenda, so it is a must that you go beyond this guide and research well. We are looking forward to having you in our committee and hope that you find this study guide helpful for your extensive research.

For any clarifications towards the Executive Board with regards to anything committee specific please feel free to get in touch with us via email to aldendsouza129@gmail.com and we will help you out. We are looking forward to an exciting committee at SJBHSMUN 2025 .

Sincerely,

The Executive Board-Commission on Crime Prevention and Criminal Justice

Alden D'Souza (Chairperson)

Arhita Sinha (Vice Chairperson)

Andria John (Vice Chairperson)

Aadidev D (Moderator)

INTRODUCTION AND COMMITTEE OVERVIEW

The United Nations Convention against Cybercrime, adopted by the General Assembly (resolution 79/243, December 2024), marks a foundational step for member states to establish comprehensive frameworks for countering cybercrime. Digital transformation has fundamentally changed crime and criminal justice, with information and communication technologies creating unprecedented opportunities for both criminals and those combating crime. The new Convention seeks to improve international cooperation, technical assistance, and capacity-building, especially for developing countries, in order to more effectively intercept and prevent cybercrime.

With 67.4% of the global population using the Internet by 2023, digital connectivity has seamlessly integrated into daily life—enabling communication, shopping, research, and innovation—but also presenting serious cybercrime risks. As a result, over two-thirds of people worldwide are now exposed to digital threats, underscoring the pressing need for robust anti-cybercrime measures.

The Commission on Crime Prevention and Criminal Justice (CCPCJ), established by ECOSOC resolution 1992/22 and designated as the governing body of the UNODC by General Assembly resolution 61/252 (2006), plays a central role in tackling these challenges. As both a policymaker and functional commission, the CCPCJ provides a forum for developing and coordinating global criminal justice strategies—now with added focus on managing digital transformation and strengthening cybercrime responses.

Technology's rapid evolution has created new opportunities but also facilitated an upsurge in cybercrime. The FBI's Internet Crime Complaint Center reported over $16 billion in losses for the most recent year, representing a 33% rise, and highlighting the urgent need for more technologically informed criminal justice frameworks.

Cybercrime's transnational nature complicates investigation and prosecution, as perpetrators exploit technology to move across borders and evade national jurisdictions—unlike traditional crimes, which are mostly confined geographically. Cybercrimes also transform familiar offenses like theft, harassment, and fraud into more complex digital variants, while new forms including ransomware and deepfakes continue to emerge. Insider threats are also growing, with 83% of businesses reporting at least one such attack in 2024.

The anonymity offered by digital platforms allows criminals to target multiple victims quickly and obscure their identities, making detection and attribution difficult. Digital evidence is highly volatile and can disappear rapidly unless law enforcement responds with proper tools and expertise. Compared to physical evidence that usually survives long periods, digital data demands swift, specialized intervention.

AI and machine learning technologies further complicate crime by equipping both criminals with new offensive tools and law enforcement with advanced detection capabilities. However, these advancements also strain criminal justice systems rooted in national sovereignty and territoriality.

The psychological effects of cybercrime are profound, especially for victims of identity theft, harassment, and privacy breaches. The financial impact extends beyond direct losses to encompass economic disruption and declining customer trust. The COVID-19 pandemic accelerated digital adoption and, unintentionally, exposed larger attack surfaces for exploitation.

Combating modern cybercrime requires integrating digital technology proactively into criminal justice systems. Digital case management can streamline court processes, facilitate seamless information sharing across jurisdictions, and reduce administrative burdens. Electronic monitoring technologies help reduce prison populations by supporting alternatives to incarceration, while digital forensics enable the recovery and analysis of electronic evidence. Predictive policing and surveillance tools—when appropriately managed—improve threat detection and crime prevention.

The United Nations has responded with several initiatives supporting member states, with the global cybercrime convention epitomizing efforts to create unified international approaches. The UNODC actively builds technical assistance and capacity-building programs. Regional bodies like the European Union, African Union, and ASEAN have established their own cooperative mechanisms, while bilateral agreements enable faster evidence sharing and joint investigations.

The private sector has a unique dual role, serving as both a key target of attacks and a critical provider of infrastructure and expertise. Public-private partnerships have proven instrumental in sharing information, setting technical standards, and managing digital evidence. International policing bodies such as INTERPOL support global best practices.

As cybercrime techniques grow increasingly complex, the need for specialized training and certification for cybercrime investigators and digital forensics experts rises. Ongoing development of these professionals is vital for effective analysis, investigation, and prosecution.

Real-time information sharing systems, such as incident reporting and threat intelligence platforms, are essential for law enforcement agencies to collaborate and rapidly respond to new threats. Such systems must balance effective information exchange with strong privacy and security protections.

With the accelerating pace of technology and rising sophistication of cybercrime, integrating digital technologies into criminal justice systems is not only an opportunity but a pressing necessity. The UN Convention against Cybercrime and the CCPCJ's strategic leadership position the international community to advance towards safer digital

societies, but success will depend on continued cooperation, partnership, and capacity-building among all stakeholders.

DEFINING KEY TERMINOLOGY AND SCOPE

1. **Cybercrime** encompasses illegal access, data interference, computer-related fraud, and content-related offences as defined by international frameworks. The Convention on Cybercrime, also known as the 'Budapest Convention on Cybercrime', is the first international treaty seeking to address cybercrime, harmonizing national laws, improving investigative techniques, and increasing cooperation among nations. It aims to deal particularly with infringements of copyright, computer-based fraud, child pornography, hate crimes, and violations of network security. Its main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering.

2. **Digital technologies** in criminal justice include AI-powered analytics, digital forensics, electronic case management and blockchain evidence systems. In today's rapidly evolving technological landscape, digital tools and analytics have the potential to facilitate access to justice, improve court procedures, and streamline digital case management systems. In addition to it, Artificial Intelligence (AI) offers promise for advanced analytics and a reduction in the administrative burden of repetitive tasks. However, these advances are accompanied by ethical concerns related to privacy, bias, and accountability. Addressing these issues requires a human rights-based approach that ensures responsible and transparent implementation of safe, trustworthy, and fair digital technologies in the judiciary.

3. **Technical assistance projects** are tailored to individual needs of beneficiary countries. The UNODC (United Nations Office on Drugs and Crime) provides technical assistance to Member States to build their capacity to prevent and control drugs, crime, and corruption. This assistance includes expertise, training, and practical tools to develop national policies and strengthen legal frameworks, and is tailored to address specific challenges in criminal justice, anti-money laundering (AML), and other areas. The process begins by conducting technical needs assessments on which to design intervention strategies, taking into account considerations such as existing strategies of national authorities, operational procedures, legal system, human and technical resources, existing approaches to interagency and regional cooperation as well as cultural and political contexts. Based on its findings, UNODC works in partnership with the beneficiary government to design and implement projects to strengthen capacity.

4. **Cybercrime** can be defined across a range of offences which have been recognized by bodies such as Interpol, Europol, the Council of Europe, the European Union, the Asia-Pacific Economic Cooperation (APEC), the Association of Southeast Asian Nations (ASEAN), the Organization of American States (OAS), the Commonwealth of Nations, the Group of Eight (G8), the Organization for Economic and Development Cooperation (OECD), to name but a few.

   Computer crime, cybercrime, e-crime, hi-tech crime, electronic crime generally refers to criminal activity where a computer or network is the source, tool, target, or place of a crime. Such crimes may be divided broadly into 2 types of categories:

   (a) crimes that target computer networks or devices directly;

   (b) crimes facilitated by computer networks or devices, the primary target of which is independent of the computer network or device.

INTERNATIONAL LEGAL FRAMEWORKS AND INITIATIVES

1. BUDAPEST CONVENTION[1]

The Budapest Convention on Cybercrime, stands as the 1st internationally binding treaty addressing cybercrimes. The Convention is designed to address copyright infringement, computer-related fraud, child pornography, and breaches of network security. It establishes authoritative investigative powers, including the ability to conduct computer network searches and intercept data.

The Convention serves as both a guideline for countries developing comprehensive national cybercrime legislation and a framework for international cooperation between signatory parties.[2] To date, sixty-one nations across Europe and globally have signed and ratified the Convention, demonstrating its widespread acceptance and implementation.[3] This harmonization is crucial as it reduces "safe havens" for cybercriminals while facilitating effective cooperation between global law enforcement agencies.

The Convention establishes four principal categories of offenses under Chapter 2, Articles 1-10.[4] First, offenses against the confidentiality, integrity, and availability of computer data systems encompass unauthorized access and interference with computer systems and data.[5] Second, computer-related offenses include fraud and forgery committed through digital means.[6] Third, content-related offenses focus specifically on child

---

[1] Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185
[2] *See id.* art. 23.
[3] *See* Council of Europe, *Parties to Treaty 185*, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.
[4] *See* Budapest Convention arts. 2-10.
[5] *Id.* arts. 2-6.
[6] *Id.* arts. 7-8.

pornography distribution and possession. Fourth, the Convention criminalizes copyright infringement conducted via computer networks.

Articles 11 and 12 address liability provisions, covering attempts, aiding and abetting, and corporate liability for cybercrime offenses. Sanctions under Article 13 include proportional punishment, potentially including imprisonment for individual offenders and criminal or monetary sanctions for corporate entities.. Notably, the Convention does not address identity theft, child grooming, spam, or cyberterrorism, representing significant omissions in its scope.

Chapter 2, Section 2 addresses digital investigation challenges by establishing six key investigative powers.[7] These include expedited preservation of stored computer data and traffic data that can identify communication transmission paths. Production orders enable authorities to compel service providers to submit subscriber information. The Convention authorizes search and seizure of stored computer data, real-time collection of computer data, and interception of content data. Service providers may be compelled to cooperate in data collection and recording processes.

Jurisdictional provisions permit parties to establish jurisdiction if offenses occur within their territory, aboard their flagged vessels or registered aircraft, or are committed by their nationals when punishable under local criminal law.

Chapter 3 establishes principles for mutual assistance in cross-border investigations. Article 23 mandates that parties "co-operate with each other to the widest extent possible," though this broad language does not expressly establish reciprocity principles. Extradition procedures under Article 24 deem Convention offenses includable in existing extradition treaties between parties, with the Convention serving as legal basis for extradition absent bilateral treaties.

Articles 27-34 establish mutual assistance request procedures, mirroring investigative powers available domestically. Article 35 mandates a twenty-four-hour contact network ensuring immediate assistance in investigations and electronic data preservation.

The Convention has been supplemented by an Additional Protocol addressing xenophobia and racism committed through computer systems, expanding its scope beyond traditional cybercrime.[8]

The Budapest Convention thus provides a foundational framework for harmonized international cybercrime legislation and enforcement cooperation, enabling coordinated responses to transnational digital threats while establishing standardized investigative procedures and mutual assistance mechanisms.[9]

---

[7] *See id.* arts. 16-21.
[8] *See* Additional Protocol to the Convention on Cybercrime, Jan. 28, 2003, E.T.S. No. 189.
[9] Research Briefing Paper on Council of Europe Convention on Cybercrime (Oct. 31, 2018). https://ppl-ai-file-upload.s3.amazonaws.com/web/direct-files/attachments/83010846/38427668-e53e-485f-9130-

2. UN Convention on Cybercrime

The United Nations Convention against Cybercrime represents a landmark achievement in international criminal law, marking the first comprehensive global treaty addressing cybercrime and the first international criminal justice treaty negotiated in over twenty years.[10] Adopted by the UN General Assembly on December 24, 2024, through Resolution 79/243 without a vote, the Convention concludes a five-year negotiation process that began with Russia's initial proposal in 2017.[11]

The Convention originated from Russia's 2017 proposal in response to perceived limitations of the Budapest Convention.[12] Despite initial opposition from the European Union, United States, and allies who viewed the proposal as potentially expanding surveillance capabilities, all 193 UN Member States ultimately adopted the treaty by consensus.[13] The negotiations involved extensive input from civil society, academic institutions, and private sector entities.[14]

The Convention aims to prevent and combat cybercrime more efficiently through strengthened international cooperation, technical assistance, and capacity-building support, particularly for developing countries.[15] The treaty is organized into nine comprehensive chapters addressing criminalization, investigation procedures, jurisdiction, international cooperation, and capacity building.[16]

The Convention mandates States Parties to criminalize four primary categories of cyber-dependent crimes:[17]

- **Confidentiality, Integrity, and Availability Offenses**: Including illegal access to information and communications technology systems, illegal interception, data interference, system interference, and misuse of devices.[18]
- **Computer-Related Crimes**: Encompassing ICT-related forgery and theft or fraud committed through technology systems.[19]

3d72527390ca/Research-Briefing-Paper-on-Council-of-Europe-Convention-on-Cybercrime-31-October-2018.pdf

[10] *U.N. Office on Drugs and Crime*, UN General Assembly adopts landmark convention on cybercrime, Dec. 23, 2024, https://www.unodc.org/unodc/en/press/releases/2024/December/un-general-assembly-adopts-landmark-convention-on-cybercrime.html.

[11] *Id.*; United Nations Convention against Cybercrime, *Wikipedia*, https://en.wikipedia.org/wiki/United_Nations_Convention_against_Cybercrime.

[12] *Id.*

[13] *U.N. News*, UN General Assembly adopts milestone cybercrime treaty, Dec. 23, 2024, https://news.un.org/en/story/2024/12/1158521.

[14] *Id.*

[15] *Supra* note 1.

[16] *U.N. Office on Drugs and Crime*, United Nations Convention against Cybercrime Chapters, https://www.unodc.org/unodc/en/cybercrime/convention/convention-against-cybercrime-chapters.html.

[17] *Id.*

[18] *Id.*

[19] *Id.*

- **Content-Related Offenses**: Specifically targeting online child sexual abuse material, solicitation or grooming of children, and non-consensual dissemination of intimate images.[20]
- **Money Laundering**: Addressing the laundering of proceeds from cybercrime.[21]

The Convention also establishes liability for legal persons and criminalizes participation in and attempts to commit these offenses.[22] The treaty grants law enforcement agencies enhanced digital investigation capabilities, including electronic surveillance, data interception, and access to stored data, subject to judicial oversight.[23] These powers are designed to address the transnational nature of cybercrime while requiring adherence to human rights obligations and due process protections.[24]

The Convention establishes robust mechanisms for cross-border collaboration, including mutual legal assistance, extradition procedures, and evidence sharing[16]. States Parties must establish a 24/7 contact network to provide immediate assistance for investigations and prosecutions.[25] The framework facilitates rapid information exchange and coordinated responses to cyber threats.

While the Convention includes provisions requiring respect for international human rights law, it has faced significant criticism from human rights organizations, NGOs, and technology companies. Critics argue that the treaty's broad definition of cybercrime could encompass any offense committed using technology, potentially facilitating digital repression and surveillance by authoritarian regimes. The Electronic Frontier Foundation and other organizations contend that the Convention lacks concrete human rights safeguards, instead providing "lip service" to human rights protections.

The Convention will open for signature at a ceremony in Hanoi, Vietnam, on October 25, 2025, and thereafter at UN Headquarters until December 31, 2026.[26] The treaty will enter into force ninety days after the fortieth instrument of ratification is deposited.[27] UNODC will serve as secretariat to support implementation and capacity-building efforts.[28]

The Convention represents a significant milestone in global cybercrime governance, providing a comprehensive framework for international cooperation while raising

---

[20] *Id.*
[21] *Id.*
[22] *Id.*
[23] *Cyberpeace Foundation*, UN Convention against Cybercrime, Jul. 17, 2025, https://www.cyberpeace.org/resources/blogs/un-convention-against-cybercrime.
[24] *Supra* note 18.
[25] *Id.*
[26] *U.N. Office on Drugs and Crime*, United Nations Convention against Cybercrime, Dec. 23, 2024, https://www.unodc.org/unodc/cybercrime/convention/home.html.
[27] *Id.*
[28] *Id.*

important questions about balancing security measures with fundamental rights protections in an increasingly digital world.

STAKEHOLDER POSITIONS AND REGIONAL PERSPECTIVES

The global cybercrime governance landscape reflects deep ideological divisions between major powers, with developing nations caught between competing frameworks while pursuing their own capacity-building priorities. These divisions manifest in two primary areas: support for existing Western-led frameworks versus advocacy for new multilateral approaches, and the balance between security cooperation and digital sovereignty protection.

Major Power Dynamics

The most significant division in international cybercrime cooperation lies between Western nations supporting the expansion of the Budapest Convention and authoritarian states led by Russia and China advocating for UN-based frameworks.[29] Western democracies, including the United States, European Union members, Australia, and Japan, have consistently positioned the Budapest Convention as the "gold standard" for international cooperation related to crimes against computers and electronic evidence.[30] These nations argue that the Budapest Convention already provides a comprehensive legal framework with 68 signatories worldwide, including strong human rights safeguards and established mutual assistance mechanisms.[31]

In stark contrast, Russia and China have rejected the Budapest Convention, viewing it as a Western-centric instrument that excludes their participation and fails to address their sovereignty concerns.[32] Russia's 2019 initiative to create a UN cybercrime convention, supported by China, Iran, Syria, Venezuela, and other authoritarian states, represents a deliberate challenge to the existing Euro-Atlantic framework.[33] China has remained outside the Budapest Convention for two primary reasons: first, signing would contradict its longstanding position that multilateral treaties should be negotiated under universal international organizations rather than regional bodies; second, the Convention's human

---

[29] See Russia and China Cheer UN Cybercrime Convention, CEPA (Aug. 20, 2024), https://cepa.org/article/russia-and-china-cheer-un-cybercrime-convention/.

[30] Explanation of Position of the United States on the Adoption of the Resolution on the UN Convention Against Cybercrime, U.S. MISSION TO THE UNITED NATIONS (May 22, 2025), https://usun.usmission.gov/explanation-of-position-of-the-united-states-on-the-adoption-of-the-resolution-on-the-un-convention-against-cybercrime-in-ungas-third-committee/.

[31] The Budapest Convention on Cybercrime: Benefits and Impact, COUNCIL OF EUROPE, at 3-5 (2020), https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac.

[32] See Anirudh Sukumar, Back to the Territorial State: China and Russia's Use of UN Treaties, 22 J. CYBERSECURITY & INT'L AFFAIRS 45, 52 (2024).

[33] Cybercrime Treaty Risks a World of UN-Sanctioned Online Control, GLOBAL INITIATIVE AGAINST TRANSNATIONAL ORGANIZED CRIME (July 21, 2024), https://globalinitiative.net/analysis/cybercrime-treaty-risks-a-world-of-un-sanctioned-online-control/.

rights provisions conflict with China's preferred approach to digital governance.[34] The December 2024 adoption of the UN Convention against Cybercrime represents a significant victory for the Russia-China coalition, despite Western opposition.[35] While the final text does not fully achieve Russia's original objectives, it establishes the principle that cybercrime governance should occur through UN processes rather than Western-led institutions.[36] The new convention's broader definition of "ICT systems" and potential for additional protocols addressing content-related crimes aligns with authoritarian preferences for comprehensive internet control mechanisms.[37]

Developing nations find themselves navigating between these competing frameworks while prioritizing capacity building, technical assistance, and technology transfer over surveillance capabilities.[38] Countries such as India, Brazil, and South Africa have emphasized that their primary concern is not the institutional venue for cybercrime cooperation but rather access to resources, training, and technology that can enhance their domestic capabilities.[39] These nations often support UN-based processes not necessarily due to ideological alignment with Russia and China, but because such forums provide greater representation for developing country perspectives and prioritize capacity building over enforcement cooperation.[40]

Regional Approaches

Regional organizations have developed distinct approaches to cybercrime cooperation that reflect their unique political, legal, and cultural contexts, creating a complex patchwork of overlapping and sometimes conflicting frameworks.

- **European Union: Comprehensive Data Protection and Cross-Border Evidence Sharing:** The European Union has emerged as the most sophisticated regional framework for cybercrime cooperation, emphasizing comprehensive data protection alongside enhanced law enforcement capabilities.[41] The EU's e-Evidence Regulation, adopted in 2023, enables judicial authorities to obtain

---

[34] *Id.*

[35] UN General Assembly Adopts Landmark Convention on Cybercrime, UNODC (Dec. 23, 2024), https://www.unodc.org/unodc/en/press/releases/2024/December/un-general-assembly-adopts-landmark-convention-on-cybercrime.html.

[36] The UN Cybercrime Convention: A Victory for State Sovereignty, AUSTRALIAN STRATEGIC POLICY INSTITUTE (Aug. 15, 2024), https://www.aspistrategist.org.au/the-un-cybercrime-convention-a-victory-for-state-sovereignty/.

[37] Confusion & Contradiction in the UN 'Cybercrime' Convention, LAWFARE (Sept. 11, 2024), https://www.lawfaremedia.org/article/confusion---contradiction-in-the-un--cybercrime--convention.

[38] Enhancing Cyber Resilience in Developing Countries, WORLD BANK (Jan. 28, 2025), https://projects.worldbank.org/en/results/2025/01/29/-enhancing-cyber-resilience-in-developing-countries.

[39] *Id.*

[40] Africa in OEWG and Ad Hoc Cybercrime Committee, DIPLO FOUNDATION, https://www.diplomacy.edu/resource/report-stronger-digital-voices-from-africa/africa-participation-international-processes-cybersecurity-cybercrime/.

[41] E-Evidence - Cross-Border Access to Electronic Evidence, EUROPEAN COMMISSION (Feb. 13, 2023), https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/e-evidence-cross-border-access-electronic-evidence_en.

electronic evidence through European Production Orders within 10 days, compared to up to 120 days for traditional mutual legal assistance procedures.[42] This system operates within strict GDPR compliance requirements, ensuring that cross-border evidence sharing maintains the EU's gold standard for privacy protection.[43] The EU approach prioritizes harmonized legal frameworks that balance investigative efficiency with fundamental rights protection.[44] European institutions have consistently argued that effective cybercrime cooperation requires not just legal mechanisms but also shared commitments to rule of law, judicial independence, and human rights protection.[45] This philosophy underlies European skepticism toward the UN cybercrime convention, which EU representatives argue lacks sufficient safeguards to prevent authoritarian abuse.

- **Asian Approaches: Balancing Crime Prevention with Digital Sovereignty:** ASEAN members have developed a distinctive approach that combines crime prevention objectives with strong emphasis on digital sovereignty protection and non-interference in domestic affairs.[46] The ASEAN Cybersecurity Cooperation Strategy 2021-2025 promotes a "multi-disciplinary, modular, measurable multi-stakeholder" approach that seeks to balance multilateral cooperation with respect for national sovereignty. This framework reflects ASEAN's traditional diplomatic culture of consensus-building and informal cooperation mechanisms.[47] Unlike the EU's legalistic approach, ASEAN emphasizes soft law instruments, capacity building, and gradual convergence of national practices rather than binding harmonization. The ASEAN Framework on Personal Data Protection encourages member states to adopt common principles while allowing exceptions that accommodate diverse domestic legal systems. This flexibility enables countries with vastly different political systems—from authoritarian Singapore to democratic Indonesia—to participate in regional cooperation while maintaining their distinct approaches to digital governance.[48] China's influence in the region has promoted emphasis on "digital sovereignty" approaches that prioritize state control over cross-border data flows and content

---

[42] *Id.*

[43] Francesco Casino et al., SoK: Cross-Border Criminal Investigations and Digital Evidence, 8 J. CYBERSECURITY 1, 8-12 (2022).

[44] Cross-Border Electronic Evidence Frameworks – EU vs. India, NATIONAL J. OF CYBER SECURITY LAW (July 7, 2025), https://lawjournals.celnet.in/index.php/njcsl/article/view/1884.

[45] *Id.*

[46] Xuechen Chen & Yihan Yang, Comparing the Approaches of the EU and ASEAN to Cyber Governance, TRANSATLANTIC INT'L STUDIES REV., at 58-62 (2022).

[47] ASEAN Cyber Diplomacy: Overcoming Differences, KASPERSKY POLICY BLOG (May 9, 2018), https://www.kaspersky.com/about/policy-blog/asean-cyber-diplomacy-overcoming-differences.

[48] Cybersecurity Governance in Southeast Asia, DCAF, at 4-6 (2023), https://www.dcaf.ch/sites/default/files/publications/documents/Cybersecurity_Governance_in_Southeast_Asia_Thematic_Brief.pdf.

regulation.[49] However, ASEAN has increasingly sought to chart a middle course between Chinese and Western models, embracing both multilateral and multi-stakeholder elements in its cybersecurity governance.[50]

- **African Priorities: Capacity Building and South-South Cooperation:** African approaches to cybercrime cooperation centre on capacity building, infrastructure development, and South-South cooperation rather than formal legal frameworks. The Africa Agenda on Cyber Capacity Building, developed by the African Union in collaboration with the Global Forum on Cyber Expertise, emphasizes regional matchmaking programs, knowledge sharing, and peer-to-peer learning among African nations.

African Regional Economic Communities such as ECOWAS, EAC, and SADC have been positioned as the primary vehicles for cybersecurity cooperation, leveraging their knowledge of specific regional needs and existing interdependent infrastructure.[51] The African approach prioritizes practical cooperation mechanisms including Information Sharing and Analysis Centers (ISACs), regional Computer Emergency Response Teams (CERTs), and Centers of Excellence for training and capacity building.[52]

South-South cooperation represents a core element of African cybersecurity strategy, with countries like Ghana, Rwanda, and Kenya serving as regional leaders in sharing technical expertise and best practices. The African Union has explicitly promoted South-South cyber capacity building as preferable to traditional donor-recipient relationships, arguing that African nations can better understand each other's constraints and develop contextually appropriate solutions.

International partnerships focus on technical assistance and resource mobilization rather than legal harmonization, reflecting African priorities for building basic cybersecurity capabilities before engaging in complex international legal cooperation. Organizations such as AFRIPOL and the AU's African Centre for Study and Research on Terrorism have been tasked with coordinating regional law enforcement cooperation while respecting diverse national legal systems and political arrangements.

---

[49] Digital Sovereignty in ASEAN, PS ENGAGE (Mar. 4, 2024), https://ps-engage.com/digital-sovereignty-in-asea/.

[50] Africa Agenda on Cyber Capacity Building, AFRICAN UNION, at 11-12 (2023), https://gc3b.org/wp-content/uploads/2023/12/Africa-Agenda-Final-Final_Dec-.pdf.

[51] Advancing Regional Cyber Security and Stability in Africa, AFRICA CENTER FOR STRATEGIC STUDIES, at 5 (2024), https://africacenter.org/wp-content/uploads/2024/06/2024-05-Cyber-RT-Executive-Summary-EN.pdf.

PROMINENT ISSUES

1. Implementation Disparities

Although digital transformation and evolution are now an integral part of effective crime prevention and criminal justice but member states differ widely in their ability and efficiency to deploy, regulate, and maintain digital technologies within judicial systems. These disparities are shaped by differences in economic capacity, development, and technical literacy. The result is a fragmented global justice system where some nations can trace cybercriminal activity across borders in seconds, while others still rely on handwritten documentation and limited connections and resources.

The United Nations Office on Drugs and Crime (UNODC**)**, through its Comprehensive Study on Cybercrime (2013) and subsequent assessments, highlights that such imbalances in global justice systems and efficiency .

2. Uneven legislative frameworks

Not all States possess comprehensive legislation addressing cybercrime. Some legal systems still depend on old, rigid definitions of theft, fraud, or intrusion that do not extend to digital contexts. Although in some countries cybercrime laws exist, many lack procedural provisions for seizing servers, decrypting data, or compelling network providers to cooperate. According to the UNODC Global Programme on Cybercrime, over one-third of surveyed countries report either no dedicated cybercrime statute or only partial coverage of offences such as illegal access or data interference.

3. Technological infrastructure gaps

Disparities in information and communication technology (ICT) infrastructure remain severe. Well-developed member states have invested in forensic laboratories, secure digital evidence storage platforms, and cloud-based case-management platforms. Conversely, many developing States depend on outdated equipment, unstable electrical supplies, and limited bandwidth. Without reliable infrastructure, digital evidence risks corruption or loss, and inter-agency data sharing becomes impractical and dangerous.

4. Human-resource shortages and skills gaps

The shortage of skilled labourers and technicians is one of the most consistent findings across UNODC assessments. Digital forensics requires multidisciplinary expertise, such as law enforcement, information technology, and legal knowledge, yet national training academies rarely offer a comprehensive curriculum. As a result, investigations into sophisticated cyberattacks are frequently delayed. The Global

Programme on Cybercrime notes that only a minority of States maintain continuous professional development for prosecutors and judges on electronic evidence handling.

5. Institutional fragmentation and siloed operations

Criminal justice institutions often function independently, with police, prosecutors, and courts maintaining completely separate databases and incompatible software. This "silo effect" prevents seamless data exchange, slows case processing, and fosters duplication of effort. UNODC technical-assistance missions consistently identify fragmentation as a principal obstacle to digital modernization.

6. **Weak international cooperation capacity**

Effective response to cybercrime depends on rapid cross-border collaboration. Yet many States lack the technical ability or efficiency to request or respond to electronic evidence inquiries. The UNODC Practical Guide for Requesting Electronic Evidence Across Borders (2019) notes that delays often arise from inadequate translation, inconsistent request formats, and the absence of 24/7 contact points. Consequently, time-sensitive evidence may be irrelevant or lost before mutual legal assistance processes conclude.

7. **Inconsistent forensic and procedural standards**

Digital-evidence procedures differ considerably according to each member state, from acquisition and chain-of-custody documentation to admissibility in court. Some jurisdictions require certified forensic images; others admit screenshots or device logs. This lack of harmonization undermines judicial confidence and prevents cross-recognition of evidence. The UNODC Electronic Evidence Hub under the SHERLOC portal has catalogued over 70 different national evidence standards worldwide.

8. **Unequal access to partnerships and private-sector collaboration**

Developed States often maintain diplomatic and strategic relationships with technology companies that facilitate lawful data access or forensic support. Developing States don't have similar cooperation, leaving them dependent on informal networks or costly commercial services. This disparity deepens the global "digital divide" in law enforcement capacity.

9. **Regional concentration of expertise**

Expertise regarding cybercrime and technology lie within a few regional hubs such as Europe, North America, and parts of East Asia, while large areas of Africa, Latin America, and small island developing States lack training centres or research facilities.

According to UNODC regional reports, the absence of localized capacity forces reliance on foreign experts, raising sovereignty concerns.

10. **Data-protection and human-rights asymmetry**

Variations in privacy legislation further complicate evidence sharing. Countries apply stringent data-protection regimes aligned with the EU General Data Protection Regulation (GDPR), while others have minimal security. These create uncertainty over wheter data can be lawfully transferred and how it must be stored, leading to inconsistent respect for individual rights.

CAPACITY BUILDING FOR CYBERCRIME PREVENTION

One of the most prevalent issues at hand is that traditional criminal justice systems lack the technical expertise and resources to effectively combat cybercrime.

"Capacity building" in the scope of the agenda is understood as enabling criminal justice authorities to meet the challenge of cybercrime and electronic evidence. This entails strengthening the knowledge and skills and enhancing the performance of criminal justice organisations including their cooperation with other stakeholders.

As the result, since the adaptation of the Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World by the CCPCJ in 2010 (Salvador Declaration), multiple strides have been made towards capacity building within Member States to improve the detection, prevention, and prosecution of cybercrime.

There are a multitude of elements to consider when we refer to capacity building

1. Legislation

The fundamental truth is that Criminal justice measures on cybercrime and electronic evidence must be based on law.

The UNODC has taken measures towards this by introducing activities like the drafting of standard operating procedures for law enforcement, creation of national strategies, guidelines, and legislation in the areas of preventing and combatting cybercrime and more

Additionally countries across the globe have also been implementing legislation for the same. This has been touched on *further up* in this document.

2. Cybercrime reporting

Limited data and knowledge on cybercrime is a key obstacle to the prevention and control of cybercrime, and makes it difficult to obtain political commitment and resources.

Reporting channels s for individuals and public and private sector Organisations such as the **International Crime Complaint** Centre and the **National Call reporting centre** are crucial as these reports often trigger law enforcement investigations, provide intelligence for a better understanding of scope, threats and trends of cybercrime, and allow for collecting data to detect patterns of organised criminality. Additional mechanisms, such as **INTERPOL's Cybercrime Knowledge Exchange (CKE)** and **EUROPOL's Internet Crime Reporting Online System (ICROS)**, are further strengthening global capacities for timely cybercrime reporting and information sharing.

3. Specialized Training of law enforcement prosecutors and judges

It is imperative that the frontline of our judicial system is able to investigate cybercrime, secure electronic evidence, carry out computer forensic analyses, assist other agencies and contribute to network security.

This is being done through multiple initiatives, specifically through the The Global Programme on Cybercrime, established by the UNODC in 2013. This programme has enhanced the skills, knowledge and abilities of **6618** criminal justice practitioners, sensitivized over 49,000 beneficiaries and engaged 376,690 children in cybercrime prevention activities.

For example, the UNODC Regional Centre for Combatting Cybercrime in Doha offers a 5 pillar approach to the general public comprising 1) specialised short-term training courses, (2) a diploma programme with a partner university in Qatar, (3) prevention and awareness-raising activities, (4) dedicated research on emerging cyber threats, and (5) mentoring programmes to build sustainability by preparing trained officials to serve as future trainers.

It also works to strengthen capacities of criminal justice practitioners and law enforcement officers on how to investigate, prosecute and adjudicate cybercrime as well as enhancing capacities of policy makers and government officials in preventing and countering cybercrime.

The UNODC, in collaboration CARICC also held a regional training on investigation of cybercrime cases in Central Asia for prosecutors from Kazakhstan, the Kyrgyz Republic, Tajikistan, Turkmenistan, and Uzbekistan, where participants were educated on plethora of topics such as cybercrime detection, electronic evidence admissibility, cryptocurrency tracing and recovery, open-source intelligence, combating crime committed via the Darknet and more.

EMERGING TECHNOLOGIES AND JUSTICE SYSTEMS

Technological innovation is revolutionizing every stage of the criminal justice process. Artificial intelligence (AI), machine learning (ML), blockchain, and data analytics are

increasingly embedded within investigation, prosecution, and judicial administration. According to the UNODC's Report on Digital Technology in Crime Prevention and Justice (2023), digital modernization can enhance transparency, accelerate case management, and strengthen the integrity of evidence collection when applied responsibly with proper oversight.

Artificial intelligence has emerged as an influential tool. Predictive analysis systems now assist investigators and judicial workers by identifying patterns in digital evidence, detecting financial anomalies, and tracing illicit networks across borders. Courts have also experimented with AI-driven document review and risk-assessment models to reduce case backlogs and increase efficiency. Yet this dependence introduces new vulnerabilities. Algorithms trained on incomplete or biased datasets can reproduce discrimination, leading to uneven or unjust judicial outcomes.

Machine learning applications in digital forensics and surveillance have advanced rapidly. Automated recognition systems can identify faces, voices, and behavioural anomalies in seconds. These systems increase investigative speed but raise privacy concerns and highlight the tension between efficiency and human rights. The UNODC and the Office of the High Commissioner for Human Rights (OHCHR) have emphasized that algorithmic transparency and human oversight are critical prerequisites for lawful use of such technologies [4].

Blockchain and distributed-ledger technologies (DLTs) have become integral to both financial innovation and digital justice. In court administration, blockchain offers the potential security to digital evidence, timestamps legal documents, and creates tamper-proof registries for case data. Its decentralized structure enhances transparency and auditability. However, the same features also empower criminals. Cryptocurrencies and privacy-oriented tokens are now central to immense money laundering operations, ransomware payments, and illicit online markets. The UNODC's Global Programme against Money Laundering reports that cryptocurrency-enabled crime exceeded several billion dollars annually by 2023, underscoring the dual-use nature of the technology.

The Internet of Things is another transformative domain. Everyday objects, such as smartphones, home assistants, vehicles, and industrial sensors, produce continuous data streams that can serve as important evidence. IoT forensics allows investigators to reconstruct timelines and corroborate testimonies, but it also presents problems of scale, jurisdiction, and reliability. Evidence may be stored across multiple servers in different countries, each governed by distinct and diverse privacy laws. *The* UNODC Education for Justice (E4J) Cybercrime Module notes that IoT evidence is volatile, easily altered by updates or network disruptions, demanding rapid preservation and specialized expertise.

Augmented Reality (AR) and Virtual Reality (VR) platforms, often referred to collectively as the "metaverse," create immersive digital spaces where users can interact through avatars and digital entities. These environments, though innovative, also enable offences

such as identity theft, harassment, and fraud in virtual form. Establishing legal jurisdiction and evidentiary standards within such spaces presents challenges. Similarly, autonomous technologies such as drones and self-driving vehicles require new frameworks of accountability. When an automated decision causes harm, determining liability between the programmer, manufacturer, and operator becomes complex and confusing.

In sum, emerging technologies are redefining justice processes. They offer powerful tools for crime detection, evidence integrity, and administrative transparency, but simultaneously create confusion between boundaries and between human judgment and algorithmic decision-making.

EVOLVING THREAT LANDSCAPE

The same technological developments that empower justice systems and the world also enable new forms of criminal behaviour. The global threat environment has grown increasingly sophisticated, borderless, and automated.

Artificial intelligence has become a weapon in the hands of cybercriminals. Deepfakes, synthetic voices, and AI-generated text allow perpetrators to fabricate convincing misinformation or impersonate officials. Fraud schemes powered by generative AI can manipulate digital identities at an unprecedented scale. The UNODC's Responsible AI Innovation in Law Enforcement (2024) report warns that such misuse erodes trust in digital evidence and weakens judicial reliability.

Ransomware continues to dominate the cyber-threat landscape. Modern attacks combine encryption, data theft, and public extortion, known as "double" or "triple" extortion models. INTERPOL's *Global Ransomware Trends Report (2023)* recorded a sharp rise in incidents targeting government and judicial institutions, with many justice networks paralyzed for weeks. Disruptions to court systems or evidence databases can compromise entire prosecutions and undermine faith in state institutions.

The expansion of blockchain-based finance has created new opportunities for criminal exploitation. Decentralized Finance (DeFi) platforms allow users to trade or lend assets anonymously, bypassing financial-reporting requirements. Money-laundering operations now move rapidly between exchanges, mixers, and privacy coins, rendering traditional asset-tracing mechanisms ineffective. The UNODC's *Crypto-Enabled Money-Laundering and the Dark Economy* (2022) report emphasizes that the absence of global regulatory consensus allows such activities to thrive.

Cloud-computing vulnerabilities pose another major risk. Many justice institutions rely on third-party service providers for data storage and communication. Misconfigurations, credential theft, or insider leaks can expose sensitive case files to unauthorized access. Attacks on software supply chains where malicious code is inserted into routine updates

have further magnified systemic fragility. UNODC analyses stress that dependence on external infrastructure without adequate oversight increases institutional exposure.

The darknet remains an adaptive criminal ecosystem. Marketplaces that once centralized illicit trade have fragmented into encrypted, peer-to-peer networks resistant to law-enforcement disruption. Transactions involving drugs, weapons, and stolen data are now facilitated through cryptocurrency escrow systems and privacy networks. Each takedown is quickly followed by re-emergence elsewhere, demonstrating the resilience of decentralized criminal platforms.

The manipulation of data for strategic gain, commonly called "data weaponization," has become a defining feature of the modern threat landscape. Disinformation campaigns target electoral systems, judicial credibility, and public trust. Synthetic content created by AI models can contaminate legitimate evidence or mislead investigations. As the UN Secretary-General noted in 2023, "the battle for truth itself has become a front line of digital conflict".

QUESTIONS A RESOLUTION MUST ANSWER

1. What universal standards and definitions should govern the integration of digital technologies across criminal justice systems to effectively combat cybercrime while respecting principles of sovereignty and diverse legal traditions?
2. How should international legal frameworks address the current divide between existing multilateral instruments (such as the Budapest Convention) and new UN-based conventions, to promote inclusive cooperation, harmonization, and trust among states?
3. What technical and capacity-building mechanisms are necessary to ensure all nations, especially developing and least developed countries, have equitable access to digital tools, training, and technology transfer, and how can these mechanisms be sustainably funded and administered?
4. What specific safeguards, oversight, and accountability processes are required to balance the efficiency of digital technologies in law enforcement and judicial functions with the protection of fundamental human rights, privacy, and prevention of technology abuse or bias?
5. How can effective regional and global cooperation be structured to address cross-border evidence collection, data protection, and enforcement, while accommodating regional priorities such as data sovereignty, data protection, and capacity building?