International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(2) 2026 pp. 1444-1459
https://doi.org/10.70917/ijcisim-2026-4251
Article

NAVIGATING THE LABYRINTH GLOBAL CYBERCRIME GOVERNANCE IN ULTRA-DIGITAL AGE

Saurabh Tewari[1], Ashok Kumar[2]

[1]Centre for Land Warfare Studies (CLAWS), RPSO Complex, Parade Road, Delhi Cantt, New Delhi -110010
Email: stewari222@gmail.com
Retired India Army officer, currently pursuing PhD from Centre for Land Warfare Studies.
[2] Centre for Joint Warfare Studies (CENJOWS), Room No 301 B-2 Wing, 3rd Floor, CGO Complex, Lodhi Road
New Delhi – 110003
Email: akumar157@gmail.com
Retired India Army officer- Defence and Media Analyst. Currently Director General, CENJOWS.

Abstract: Cybercrime is global by nature as it traverses on the internet. It sees no international boundaries, and herein lies the problem. The trans-border nature of cybercrime gives it a totally different dimension that renders traditional crime investigation techniques and procedures redundant. While new age technologies make our daily lives simpler and more efficient, they also provide the cyber-criminals a wider canvas to operate upon. Law enforcement is always playing a catch-up game with the cyber-criminals on the technology front. Footprints of a typical trans-border cybercrime may lie in multiple countries; this gives rise to difficult questions like which country's territorial jurisdiction will apply, victim or accused? Which country's cyber law will apply, victim or accused? How to ensure that digital evidence in a third country does not get tampered before it is seized by law enforcement? How to trace the computing machines (that have been used by cyber-criminals) across the globe and seize them? How to transfer digital evidence to another country? These are questions that are difficult to answer today. Global cybercrime governance plays a major role in providing a framework for resolution of such complex situations. This paper attempts to study the existing global cybercrime governance framework and suggest measures to strengthen the same, to reduce the trans-border cybercrime globally and enhance conviction of cyber-criminals, irrespective of their country.

Keywords: Budapest Convention-2001, Cybercrime, Dual-Criminality, Global Cybersecurity Index, International Criminal Police Organisation (INTERPOL), Tallinn Manual, UN Convention Against Cybercrime-2024, UN Office on Drugs and Crime (UNODC)

1. INTRODUCTION

We live in an extremely interconnected world, where we have learnt to live with cybercrime and data privacy violations. With Information and Communication Technologies (ICT) invading our lives, the threat emanating from cybercrimes has evolved into a full-blown global issue that is threatening not only individuals, but also enterprises and governments alike.

Ubiquitous proliferation of high-tech cyber-attacks, ransomware threats, financial frauds, child pornography, data theft, business espionage and state sponsored cybercrimes/espionage, etc has reached a tipping point, where a dire need is being felt by all for an effective global cybercrime regulatory framework. As technology is advancing, novel cybercrime methods are evolving, leaving the Law Enforcement Agencies (LEAs) across the globe playing catch-up. Criminal use of any technology is the first to take-off; good uses generally take time to fructify. Recent cyber-attacks like data breach on Tata Electronics in Jun 2026, attacks on website of Election Commission of India in Apr 2026, the attack on Singapore telecom network by a Chinese hacker group in Feb 2026, lockdown of AZ Monica Hospital servers in Belgium in Jan 2026, the attack on Paraguay health ministry in Jun 2025, stealing of $81 million cryptocurrency from Iranian crypto exchange in Jun 2025, attack on X (Twitter) in Mar 2025, hacking of Polish Space Agency in Mar 2025 and attack on Bybit crypto-currency exchange in Feb 2025, leading to loss of $1.5 billion, make us realise how vulnerable our equipment and systems are. These cybercrimes lead to breach of sensitive data,

operations disruption, fiscal damage and smeared reputations. Phishing attacks, Denial of Service (DoS) attacks and financial frauds are scaling new heights targeting citizens, governments and businesses alike. Ransomware attacks have also seen an unparalleled rise in last few years; in fact, ransomware-as-a-service is the latest trend in cybercrime circles (typically using a malware called Satan)- that is, one could hire a hacker to perform a ransomware attack, with a fees. Commercial malwares are available on the dark-web for sale and even social media account hacking is available for as low as $450 per account. Hacked personal information is available for anything between $10 to $4000 depending on how sensitive it is. In this paper, an attempt has been made to analyse the existing global cybercrime governance framework and comment on its adequacy and efficacy in management of trans-border cybercrimes. In doing so, it is also intended to suggest measures to strengthen the framework through a unified approach, to build a safer digital future for the global community.

1.1 Trans-Border Cybercrimes

Trans-border cybercrimes present a unique challenge to LEAs and judiciary all over the world. Disparate legal frameworks and investigation mechanisms, differing cybercrime definitions, etc create large loopholes for cyber-criminals to exploit. If the criminal and target machine/victim(s) are not in same country, issues regarding jurisdiction crop up- which country's jurisdiction shall apply? Criminal or the victim? Does the act classify as a crime in both countries (aspect of dual-criminality)? Are legal procedures harmonised between the two countries? Do both countries have mutual assistance treaty and extradition treaty? If digital evidence is not examined/collected in an early time frame there is a good probability that it might get tampered with. Consequently, judicial convictions in trans-border cybercrime cases are far and few; most of such cases remain unresolved for years. These are complex issues that need resolution if any headway is to be made in adjudication process. However, as it stands today, these are totally grey areas and need urgent attention of all stake-holders.

1.2 Global Cybercrime Footprint

It is commonly understood that trans-border cybercrimes are geographically widespread across the globe. However, this is far from true. A study conducted in 2024 shows that most of the cybercrimes are concentrated around few countries. Top 10 global cybercrime hubs that emerged in this study (in the order of their rank, starting from first) are "Russia (58.39), Ukraine (36.44), China (27.86), US (25.01), Nigeria (21.28), Romania (14.83), North Korea (10.61), UK (9.01), Brazil (8.93) and India (6.13)" . The figure given in brackets with each country is the score out of 100. The study also analysed the types of cybercrimes originating from these countries; it emerged that Russia tops the list for cybercrimes related to technology, digital attacks, ransomware extortion, identity theft, data breach and financial crimes, while Nigeria leads the list for cyber-scams. The study clearly shows that cybercrime hubs are concentrated across just a handful of countries and not spread far and wide across the globe. The outcome of this study is also being used by global bodies like the United Nations (UN), International Criminal Police Organisation (INTERPOL) and International Telecommunication Union (ITU), to devise specific strategies and focus their efforts towards these countries.

1.3 State Sponsored Cybercrime & Cyber-Attacks

Involvement of state sponsored actors presents a totally different paradigm to the concept of cyber-attacks. Over the last decade, global instances of state-sponsored cyber-attacks have been on the rise. As per a report, state-sponsored cyber-attacks amounted to 35 per cent of all attacks globally and there is an increasing trend of state sponsored attacks on national critical infrastructure. While there are global conventions addressing the issues regarding cybercrimes (like the Council of Europe's (CoE) Convention on Cybercrime-2001 or the UN Convention Against Cybercrime-2024), there are no conventions/regulations pertaining to inter-state cyber warfare. An attempt to study the relevance of international/global law in inter-state cyber warfare was made by the North Atlantic Treaty Organisation (NATO) in 2013, resulting in a document called the Tallinn Manual; a revised version 2.0 was further issued in 2017. Recent cases of state sponsored cyber-attacks and inter-state cyber warfare include the attack on Indian Defence educational institutes by Pakistan based hacker group in April 2025, the ongoing cyber-attacks by Russia and Ukraine on each other since February 2023 and the cyber-attacks by Israel and Iranian on each other's critical infrastructure in June 2025. However, it is important to understand that the Tallinn Manual is just a compilation of recommendations of a group of government, industry and academic experts, and is in no way binding on any state government, and neither represents views of the NATO. Inter-state cyber conflict between Israel and Iran is a latest classic example of dangerous trends in global cyber warfare; these include use of latest sophisticated malware, AI assisted attacks, supply chain infection, convolution of cyber and physical war, extending beyond military targets to critical infrastructure like finance, manufacturing, energy, water, aviation and maritime. Documented attacks include the attack on South Pars

gas field (joint venture of Iran and Qatar) and the Haifa Refinery (owned by Israel), attacks on Iran steel manufacturing facilities by Israel based hacker group Predatory Sparrow, disruption of Shahid Rajaee port (Iran), DDoS attacks on Society for Worldwide Interbank Financial Telecommunication (SWIFT) systems by Iran backed hacker group APT34 and Israel based cyber-espionage company Candiru. Such cyber-attacks on critical infrastructure adversely impact the country's economy, erodes public trust in governance and in some cases may lead to physical destruction and loss of lives also.

1.4 Impact of Cybercrimes

Economic impact of cybercrimes is immense. As per a report, cybercrime costs between Jan-May 2026 have already reached $1.2 trillion, with productivity loss pegged at $1trillion, and cybercrime costs are likely to touch $15.6 trillion by 2029. If cybercrime industry were a country, it would rank third largest economy after US and China, ransomware industry will reach $265 billion in 2031 and global cyber-security industry will reach $425 billion by 2027. In terms of GDP, annual cybercrimes costs are already touching 2.5% of the global GDP, which is a serious matter. However, repercussions beyond the financial costs are also significant; for example, attacks on healthcare or water supply systems can erode public confidence in governance, a data breach in business house can irreparably damage its market reputation and mar business opportunities, an attack on a nuclear facility can lead to radiation leakage causing loss of lives, hack on smart autonomous vehicle systems can lead to accidents on the roads, cyber bullying or fake porn videos can mentally scar a child for life, and so on. All these negative effects can make technology adoption sluggish and unwanted by the general public. The consequences of a cybercrime or cyber-attack are wide spread in geography and impact domains; they could also have social implications like inciting riots, individual embarrassment, mental agony, etc. Implications on national security are also severe; state sponsored cyber espionage activities or attacks on critical infrastructure like telecom, banking & finance, railways, maritime, aviation, defence, etc can put back a country by several decades. Indulgence in election rigging, hacking of defence infrastructure could also escalate geo-political frictions.

1.5 Impact of New Age Technologies

While the advent of new age technologies is making life simpler and more efficient for the citizens, government and businesses, it is providing two distinct advantages to the cyber-criminals; one, by creating larger cybercrime landscapes, and two, by providing cyber-criminals with new technologies to evade detection and prosecution. The more online services are pushed to the common man, the more vulnerable he is to cybercrime. Technologies such as Internet protocol (IP) spoofing, Virtual Private Networks (VPNs) and The Onion Router (TOR) provide a shroud of secrecy and un-traceability to these hackers. They sit in countries that have weak legal frameworks, and execute cybercrimes with confidence, understanding quite well that the legal loopholes and technology assisted obscurity will save them from any negative implications. A cyber-criminal sitting in US can take control of a laptop in Singapore, use it to launch a cyber-attack on a bank server in India and deposit the crime proceeds in a bank in Cayman Islands; and in between, the hacking traffic (IP packets) will hop across multiple servers across the globe. In such a scenario, it is next to impossible to trace the origin of the crime, and even if it traced, there are other complexities to handle like territorial jurisdictional issues, establishing dual-criminality, differing cyber laws, complex procedures to request for digital evidence collection and extradition of the accused. Further, new concepts like the cryptocurrency, quantum computing, Artificial Intelligence (AI), blockchain, smart homes, Internet of Things (IoT) provide newer opportunities to cyber-criminals. As of May 2026, there has been a 659 percent increase in crypto-jacking attacks and 20 percent increase in ransomware attacks on industrial control systems (year-on-year) including Operational Technology (OT) systems. Cyber-criminals are employing innovative ideas like key logger, voice cloning, deep fake video, fingerprint cloning, biometric cloning, etc to commit cybercrime.

The peculiarities of cybercrimes/ cyber-attacks discussed above underscore the need for a custom-made global governance framework. The nuances of traditional crimes are far different and apropos, the traditional mechanisms available today to tackle trans-border traditional crimes may not suffice to contain the menace of trans-border cybercrimes. In the next section we shall study the existing global cybercrime framework, including its efficacy and adequacy, followed by recommendations to improve the same.

2. GLOBAL CYBERCRIME GOVERNANCE FRAMEWORK

Global cybercrime governance refers to the policies, guidelines, processes, procedures and regulatory frameworks that help the global community, especially the LEAs and judiciary, to investigate and adjudicate trans-border cybercrimes, as also help in strengthening the ecosystem with a special focus on developing and under developed countries. While there are no globally binding regulations, there exist some conventions and model laws

that act as guidelines for resolution of trans-border cybercrimes. In this section we shall discuss the various global organisations, policies, conventions and assistive regulatory frameworks that are contributing to our fight against cybercrime.

2.1 International Efforts

Global and regional bodies like the UN, ITU, INTERPOL, Council of Europe (CoE), European Union (EU), Organisation for Economic Cooperation and Development (OECD), African Union (AU), and NATO have made continuous efforts since early 1980s to bring more harmony amongst nation states and strengthen the global cyber ecosystem, as given below:

Between 1983 and 1985, the OECD studied the possibility of harmonizing the cyber laws of various countries and highlighted the challenges in achieving the same.

In 1989, CoE adopted Recommendation 89(9), highlighting the need for harmonizing cyber laws of nation states.

In 1994, UN published the Manual on the Prevention and Control of Computer Related Crime.

In 1995, Recommendation R(95)13 was adopted by the CoE, which provided guidelines for investigation actions like search, seizure of digital evidence, etc.,

In 2001, CoE prepared the Convention on Cybercrime at Budapest which came into effect in 2004 (hereinafter called the Budapest Convention-2001).

In 2004, Cooperative Cyber Defence Centre of Excellence (CCD-CoE) was established by NATO to provide assistance to NATO countries in cyber research and regulatory issues.

In 2007, ITU started a program called Global Cybersecurity Agenda, providing a structure for global collaboration and increasing assurance in an information based society.

In 2011, and later in 2015, China and Russia made a draft global cybercrime regulation and presented to the UN. However, UN did not agree to it as it included contentious issues like state-control of the internet.

In 2011, an Open-ended Intergovernmental Expert Group on Cybercrime was set up by the UN Office on Drugs and Crime (UNODC), followed by a program called the Global Program on Cybercrime in 2013, with the aim to help member states to strengthen their framework in fight against cybercrime.

In 2013, European Cybercrime Centre (EC3) was set up by the EU to work as a nodal agency for all aspects related to cybercrime and cyber security.

In 2013, a guideline document, called the Tallinn Manual, was prepared by a committee of experts under the aegis of NATO, which laid down interpretation of applicability of global laws in case of inter-state cyber warfare.

In 2014, AU adopted the Malabo Convention, a regulatory framework for cybercrime and protection of digital personal data. ,,

In 2017, NATO revised the Tallinn Manual and published Version 2.0.

In 2018, General Data Protection Regulation (GDPR) was promulgated by the EU. This was the first personal digital data protection act across the globe.

In 2021, UNODC published the report of the Open-ended Intergovernmental Expert Group on Cybercrime, founded on the group's deliberation from 2019 to 2021. This report highlighted very critical recommendations for strengthening the cyber framework across the globe.

In 2022, EU launched the "Global Alliance Against Child Sexual Abuse".

In 2024, Cyber Resilience Act was adopted by EU with the aim to ensure cyber security in all products (including software) that have digital components. This was quickly followed by the Digital Operational Resilience Act that provides for a strong framework for financial sector digital security.

In 2024 end, UN General Assembly (UNGA) approved the UN Convention Against Cybercrime, which was the result of deliberations for over five years between all stakeholders (hereinafter called the UN Convention-2024). The Convention is currently open for signatures by member countries.

The activities listed above progressively led to more coherent thinking on the subject of cybercrime amongst countries and global/regional bodies. However, much more is required, specifically in signing of a common framework like the UN Convention-2024. The biggest advantage to cyber-criminals has always been the trans-border nature of cybercrime, which they keep exploiting, thus managing to evade the law. A common framework of understanding between nation states is only the first step towards curbing this exponentially growing menace. We shall now study the various international/regional organisations and conventions, and discuss their efficacy and adequacy in the present context.

2.2 International Telecommunications Union (ITU)

In May 2007, ITU initiated the Global Cybersecurity Agenda (GCA), with the aim to set up a framework for harmonizing international response to cybercrime. In furtherance of this aim, ITU also started the Global Cybersecurity Index (GCI) rankings in 2015, which continues till now (last one being done in 2024). ,

2.3 European Union (EU)/ Council of Europe (CoE)

EU and CoE have both been very active in combatting cybercrime and safety of personal digital data. With a slew of measures taken since 2001, EU and CoE have been in the forefront. The first ever cybercrime treaty, called the Convention on Cybercrime (Budapest Convention-2001) was drafted by the CoE in Budapest 2001, which laid the groundwork for harmonization of global cyber regulations. Three years later, in 2004, the European Network and Information Security Agency (ENISA) was set-up to ensure high level of cyber security for government and private organisations; ENISA is now called the EU Agency for Cybersecurity. In 2011, a framework was established to fight online sexual exploitation of minors and in 2013, the European Cybercrime Centre (EC3) was established. General Data Protection Regulation (GDPR) was promulgated by the EU in 2018. EU launched the Global Alliance Against Child Sexual Abuse in 2022. The Cyber Resilience Act was adopted by EU in 2024 with the aim to ensure cyber security in all products (including software) that have digital components. This was quickly followed by the Digital Operational Resilience Act aimed to provide enhanced cyber security to the financial sector.

The Budapest Convention-2001. Budapest Convention-2001, drafted by the CoE is a guide to "facilitate detection, investigation and prosecution of cybercrimes at domestic and international level and provide arrangement for fast and reliable international cooperation". Its main focus is on global cooperation and includes a large number of cybercrimes like unlawful interception, unlawful access to computers, misuse of computers, online fraud, electronic forgery, IPR violations and child porn. The Convention became operative in 2004 and as of Jul 2026, 82 countries have ratified and signed it; in addition, 15 countries are observers. Few big countries like Russia, China and India have not ratified asserting that they did not participate in the process of drafting the Convention. In addition, Article 32 of this Convention which provides access to cross-border data without host's consent, is deemed contentious. There have been two amendments to this Convention, once in 2003 and then in 2022; the first amendment included cybercrimes related to racism & xenophobia and the second amendment provided framework for cooperation by telecom service providers in crisis situations and security of digital personal data.

Analysis. Till Dec 2024, the Budapest Convention-2001 was the only global convention available that addressed the trans-border nature of cybercrime. However, post adoption of the UN Convention-2024 by the UNGA, its relevance has reduced. Further, the Budapest Convention-2001 does have some grey areas as given below:

Some important cybercrimes that it does not include are incorporeal property theft, piracy of software/music/films, ransomware, cyber-attack against critical infrastructure, online gambling, catfishing, cyber bullying, cyber terrorism and personal identity theft.

Drafted more than two decades back, the Convention is technically obsolete, and fails to take into account new-age technology issues like cloud services, Internet of Things (IoT), autonomous vehicles, quantum computing, blockchain, crypto-currency frauds, digital arrest, deep fake video, audio cloning, AI enabled cybercrimes, use of TOR network, etc.

The non-EU countries have often criticized the Budapest Convention-2001 for it western centric approach. Some, like Russia, even view it as a threat to their sovereignty. Article 32 of the Convention provides unhindered access to data without consent of the host nation. It states:

"A Party may, without the authorisation of another Party, (a) access publicly available (open source) stored computer data, regardless of where the data is located geographically, or (b) access or receive, through a computer

system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system."

This is a contentious clause that could have been avoided, and has been a major reason for some important countries not to ratify/sign the Convention, including Russia, China and India.

The incongruence in commitment levels of various member countries in implementing the stipulations of the Convention also poses challenges by creating inconsistent efforts and legal loopholes. Apropos, the full potential of Budapest Convention-2001 is yet to be realized, pending complete commitment of all member countries in this domain.

Budapest Convention-2001 is not a lawfully binding convention; compliance is on volunteer basis. Some excerpts from the Convention to substantiate this are given below:

"Each Party may reserve the right not to apply or to apply only in specific cases or conditions."

"Extradition shall be subject to the conditions provided for by the law of the requested Party."

"Mutual assistance is conditional upon the existence of dual criminality."

"Reserve the right to refuse the request for preservation if the condition of dual criminality cannot be fulfilled."

"Any Party may, at any time, denounce this Convention by means of a notification addressed to the Secretary General of the Council of Europe."

A study was conducted to assess the cybercrime occurrence in various countries before and after signing the Budapest Convention-2001. The study clearly established that cybercrime incidents reduced by almost 30% post the signing of the Convention, thereby highlighting the positive impact of global cooperation and collaborative regulatory frameworks. Countries who have not yet signed the Budapest Convention-2001, now have the option to ratify/sign the UN Convention-2024 instead, which has a better global acceptability, being a UN drafted document. This makes a strong case for all countries to sign the UN Convention-2024 at the earliest.

2.4 UN Office on Drugs and Crime (UNODC)

Under the UN, UNODC is the primary body dealing with aspects related to drugs and crime. Cybercrime also falls under the purview of UNODC. Headquartered in Vienna, it is responsible to help and assist member nations in their fight against cybercrime, through its offices at 130 locations across the globe. Notable initiatives undertaken by the UNODC towards this aim include publishing of the UN Manual on Prevention and Control of Computer Related Crime in 1994, setting up an Open-Ended Intergovernmental Experts Group on cybercrime in 2011, initiating the Global Program on Cybercrime in 2013, publishing the Experts' Group Report in 2021 and preparing the UN Convention-2024.

2.5 UN Manual on Prevention and Control of Computer Related Crime

This Manual, the first of its kind by any global or regional body, was published to establish a common framework for all nations to understand the global implications of cybercrime. It provides details on various types of cybercrimes, applicability of traditional laws on cybercrimes, need for harmonization & international cooperation required to solve trans-border cybercrimes (to include aspects of territorial jurisdiction, trans-border digital evidence examination and seizure, mutual assistance, extradition of the accused, *etc*.), the criticality of training of LEA and judicial officers on technical matters related to cybercrime, aspects of victim cooperation, etc. This Manual was not intended to be signed by any member states, but was intended to serve as a guideline document only. The Manual is now outdated being three decades old and has lost its relevance with the adoption of new UN Convention-2024.

2.6 Open Ended Intergovernmental Expert Group on Cybercrime

This experts' group was set up to conduct study on all aspects of cybercrime and make recommendations on strengthening of cyber regulations. The group had several meetings between 2011 and 2020, and published a report in 2021. Major recommendations were as follows:

Cyber regulations must be drafted in a manner to make them technology agnostic.

National cyber regulations must cater for global cooperation in case of a trans-border cybercrime and member states must set up nodal organisations and a fast track response mechanism to assist the same.

Dedicated cybercrime units must be set up by all member states.

LEAs and judiciary must be provided with specialist training to handle cybercrime cases.

All member states should endeavour to raise cybercrime awareness amongst common public and actively involve the industry to find solutions.

A globally accepted common regulatory framework is required to be developed by the UN (it is this recommendation which triggered the process of drafting of the UN Convention-2024).

2.7 Global Programme on Cybercrime

UNODC started this program in 2013 as approved in UNGA Resolutions 65/230, 22/7 and 22/8. Funded by the Australia, Canada, Japan, Norway, UK and the US, the main purpose of this program was to help member nations to develop capability and provide technical assistance to manage cybercrime. A report was published in 2013 which gave some very pertinent observations. The major highlights are given below:

There is inadequate coherence in national cyber laws of all countries leading to varying legal interpretations & territorial jurisdictional conflicts, and this fact is being exploited by the cyber-criminals to evade conviction.

Traditional means of evidence collection are not suited for trans-border cybercrimes as digital evidence has very low shelf life and is highly prone to tampering.

In a digital era driven by cloud infrastructure-based services like computing and storage, the concept of physical location of evidence needs a review.

2.8 UN Convention Against Cybercrime-2024

On 24 December 2024, UNGA adopted the Convention Against Cybercrime. This day has also been declared by the UN as International Anti-Cybercrime Day. The UN Convention-2024 was drafted over a period of five years with detailed deliberations and consultations between all member states and other stakeholders. It is open for signatures till end 2026 and is deemed to be effective 90 days after signatures by at least 40 countries. As of Jan 2026, 72-member states have signed, and hence the Convention is already "in effect". This Convention is different than the Manual earlier issued in 1994, as the manual was only a guideline and not intended to be ratified & signed by member states. Through this Convention the UN is targeting to provide common definition to various terms connected with cybercrime/cyber security, harmonize the cyber regulatory framework and mutual legal assistance between member nations, enhance international cooperation in trans-border investigation & evidence examination/collection, digital evidence and data preservation, freezing of crime proceeds, witness protection, extradition of accused, capacity building for weaker nations, dual-criminality, handling of personal data, setting up of 24x7 helpline and inter-LEA communication channels by each member state, increased focus on public-private-academia partnership, spreading awareness amongst common public, training of LEA and judiciary in technical aspects, encouraging research, increasing availability of cyber security professionals, online safety of minors, etc. The major cybercrimes that are part of the Convention are:

- *"Illegal access and interference to computers"*
- *"Illegal data interception"*
- *"Misuse of computer device, digital signature, etc. for cybercrime"*
- *"Forgery, theft related to ICT systems"*
- *"Online abuse and exploitation of minors"*
- *"Money laundering, illegal online sale of weapons, drugs, etc."*
- *"Cyber terrorism"*
- *"Intellectual property Right (IPR) theft"*

Analysis. On detailed analysis of the UN Convention-2024, it emerges that it suffers from certain drawbacks, as discussed below:

The definitions provided in the manuscript are not comprehensive. It would be beneficial to include additional key terms such as asymmetric cryptographic system, cloud computing service, computer trespasser, critical infrastructure, digital signature, public/private key, and protected computer to improve the completeness and clarity of the content.

Similarly, the coverage of cyber offences can be expanded to include important contemporary cybercrimes such as cryptocurrency-related crimes, ransomware, software and music piracy, the use of deepfake audio and video in cybercrime, digital arrest scams, cyberattacks against critical infrastructure, identity theft, online gambling, the propagation of xenophobic or racist material over the internet, and the misuse of the TOR network.

The impact of use of AI based tools and other new technologies/concepts like cloud services, IoT, autonomous vehicles, quantum computing, blockchain, crypto-currency frauds, digital arrest, deep fake video, audio cloning, AI enabled cybercrimes, use of TOR network, etc. on cybercrime should be included, as these technologies provide a totally new dimension to cybercrime execution.

However, despite the above deficiencies, the UN Convention-2024 is still a very progressive step towards harmonizing global efforts in fight against cybercrime. The Budapest Conevtion-2001, which is the only other global convention in this domain, has been signed by only 82 nations (despite being 24 years old). Hopefully, the UN Convention-2024 will do better as it was prepared over a protracted duration of time, with detailed discussions with all member states of the UN, thereby leading to better credibility and wider acceptability.

2.9 International Criminal Police Organisation (INTERPOL)

International Criminal Police Organisation (INTERPOL) is a global organisation having 195 member countries. Its aim is to help LEAs of member countries in crime investigation and sharing of database. The Cybercrime Directorate within INTERPOL handles all cases related to cybercrime. A National Central Bureau (NCB) is nominated by each country as the Single Point of Contact (SPOC) for interaction with INTERPOL and other NCBs. INTERPOL has overall three programs, including one on cybercrime, *viz* Organised and Emerging Crime, Counter-Terrorism and Cybercrime. A National Cybercrime Strategy Guidebook was issued by the INTERPOL in April 2021; it includes guidelines for all countries to develop their own robust cyber strategy. In 2022, INTERPOL has also published a Global Cybercrime Strategy to help all countries in their fight against cybercrime; this Strategy document includes important aspects like threat analysis, data exploitation, digital evidence examination/collection and global cooperation.

Services Provided by the INTERPOL. INTERPOL provides critical services for resolution of cybercrimes as given below:

- Cybercrime Collaboration Services. INTERPOL maintains a database specific to cybercrime issues which is accessible to all member countries. In addition, it has a well-established framework for collaboration by multiple LEAs involved in investigation of trans-border cybercrimes.
- Cybercrime Threat Response. INTERPOL runs a Cyber Fusion Centre in which industry and LEA experts meet for knowledge sharing and to work out solutions and guidelines for cybercrime management.,
- INTERPOL Databases. A total of 19 databases are maintained by the INTERPOL which are accessible to LEAs of all member countries, as per details given below:
    - ✓ Notices that pertain to fugitives and missing persons.
    - ✓ Criminal databases pertaining to their criminal history, including child abuse and terrorist activities.
    - ✓ Forensics database comprising of fingerprints, face images, DNA, etc.
    - ✓ Travel and official documents database that includes identity frauds, stolen government documents, forged documents, etc.
    - ✓ Stolen property database that includes identity of all stolen vehicles, maritime vessels, and artworks.
    - ✓ Firearms Trafficking database that comprises of firearms and ballistics details.
    - ✓ Organised Crime database that includes maritime piracy details.

INTERPOL Projects. INTERPOL is also running a large number of projects that help member countries in managing cybercrimes. These projects are discussed below:

- "Speaker Identification Integrated Project (SIIP)-2014", which uses voice samples to identify criminals.
- "Managing Alternatives for Privacy, Property and Internet Governance (MAPPING) Project-2015", that provides a platform for experts' discussions on various aspects of crime.
- "European Informatics Data Exchange Framework for Courts and Evidence (EVIDENCE) Project- 2015", that explores application of new age technologies in collection of digital evidence.
- "Cyber Capabilities & Capacity Development Project (C3DP)- 2016", that aims to enhance LEA capabilities in all aspects of cybercrime.
- "Project Titanium- 2017", that develops tools for use in investigation of all crimes related to virtual currency.
- "Project EVIDENCE-2 e-CODEX- 2018", that lays down a framework for sharing of electronic evidence within the EU.

2.10 North Atlantic Treaty Organisation (NATO)

NATO has also taken few initiatives towards managing global cybercrime. In 2004, NATO established the CCD-CoE, with a mission to "enhance the capability, cooperation and information sharing among NATO nations and partners in cyber defence by virtue of education, research and development". CCD-CoE is headquartered in Tallinn, Estonia and lends support to NATO states in research and training as pertains to cybercrime. CCD-CoE also runs the CyCon, which is an annual global conference of cyber experts from government, academia and industry.

The Tallinn Manual. CCD-CoE published the Tallinn Manual in 2013. It was drafted through consultations with a large group of experts from regulatory, technical and legal domains. It discusses application of international regulations to inter-state cyber warfare, and is not related to cybercrime per-se; for example, cyber-attack on the critical infrastructure of one country by another. This Manual is only a guideline document and not legally binding on anyone, neither it represents the views of NATO. The revised document, Tallinn Manual 2.0, was published in 2017.

2.11 Shanghai Cooperation Organisation (SCO) Agreement

The "Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization" was signed on June16, 2009. The SCO was constituted on June 15, 2001; it has nine members (India, Iran, Kazakhstan, China, Kyrgyz, Pakistan, Russia, Tajikistan and Uzbekistan) and three observer members (Afghanistan, Belarus and Mongolia). The SCO Agreement talks of cooperation in the domain of information security, including aspects of cybercrime, cyber-terrorism, as well as information warfare weapons. Other than the Tallinn Manual, this is probably the only international document that talks of use of information weapons by nations against each other. The important cooperation aspects that this Agreement dwells upon are implementation of joint measures for ensuring information security, creating a monitoring and implementation system for cooperation, limiting the use of soft weapons that threaten state security and communal safety, countering cybercrime and cyber-terrorism, misuse of information dominance by one country against others, information warfare through misinformation, cyber research, safety of critical infrastructures, trans-border information exchange and interaction with other global organisations.

2.12 Other Initiatives

In addition to above, there are plethora of programs by various non-governmental organisations across the globe that are working towards containing the menace of cybercrime. These are discussed below:

Anti-Phishing Working Group (APWG). The APWG is a group of people from the industry that fights against phishing and spoofing through development of security standards and response protocols.

European NGO Alliance for Child Safety Online (eNACSO). eNACSO is funded by the EU and works towards online child protection by sharing best practices and policies with all European countries.

International Association of Internet Hotlines (INHOPE). INHOPE is a group of non-profit organisations across the globe that works to deter the online proliferation of child pornography, by establishing hotlines that continuously report illegal online content.

Internet Watch Foundation (IWF). IWF is based in the UK and works towards removing online child pornography content, in coordination with LEAs.

SpamHaus. This organisation is based in Geneva and London, and works towards detecting real time cyber threats and informing the same to government, cyber security industry and network providers.

3. CHALLENGES

Challenges to solving trans-border cybercrimes are many; jurisdictional disputes, new technologies, diverse regulatory frameworks, vulnerabilities of networks and systems, state sponsored hacker groups, regulatory compliance gaps, etc. these are discussed in detail below.

3.1 Trans-Border Nature of Cybercrimes

The cybercrime governance framework, as prevalent today, has been discussed in detail above. Trans-border cybercrimes offer very distinctive challenges to LEAs and judiciary across the globe. In contrast to conventional crime, the accused, victim and evidence in a trans-border cybercrime sit in multiple countries. such trans-national crimes exploit the gaps in regulatory frameworks of multiple nations, to evade law. There are a large number of cybercrime cases that are still unresolved due to trans-border issues. For example, the case of cyber espionage against Russian hacker Evgeny Bogachev is pending since 2009, the Yahoo data breach case is pending since 2013, the Wannacry ransomware case is pending since 2017, and so on. Management of such crimes therefore call for a totally different approach as compared to traditional crime; one that can provide a unified response across the international borders. Efforts to address this unique challenge have been made by world bodies over a period of last 24 years, starting with the drafting of Budapest Convention-2001 by the CoE. Other bodies like the UN, ITU, INTERPOL, etc have been making their own efforts over a protracted duration. However, there is still a long road to be covered; treaties like the Budapest Convention-2001 have had limited acceptability in the global platform as it was a regional effort led by the CoE and major countries did not participate in the consultative process (that includes Russia, China and India). since only 82 countries have signed the Budapest Convention-2001, it leaves almost 60% of the UN recognised countries out of its ambit, thereby defeating the purpose. Notwithstanding the grey areas in global cybercrime governance, there have been success stories also in cracking global cybercrime syndicates; one such success story is dismantling of the Avalanche network, which was operative since 2009 and provided services like mass malware proliferation, phishing attacks, redistribution of laundered money across international borders and even provided botnets for DDoS attacks; the victims of such services were spread across 180 countries and 500,000 infected computing machines. The losses on account of these cybercrimes were estimated at €6 million in Germany alone and few hundred million euro, worldwide. The investigations started in 2012 with involvement of multiple agencies like INTERPOL, FBI, German police, Europol and LEAs of about 30 countries. The investigation carried on for four years before success was achieved in Dec 2016, when more than 800,000 domains and 121 servers were seized/blocked.

3.2 Weak Framework in Under-Developed Countries

Another issue is the capability development in undeveloped and developing nations in their battle against cybercrime. As it is said, the chain is as strong as the weakest link. If under-developed countries lag behind, they provide safe-havens to the cyber-criminals by exploiting their weak regulatory framework to commit cybercrime with impunity and take refuge behind the weak ecosystem. Apropos, even countries having strong cyber ecosystem can be impacted in such a scenario. It therefore implies that unless the complete international community works with a unified approach on improving the system, everyone suffers. Assistance by developed countries to strengthen the cyber ecosystem of under-developed/ developing countries should therefore be an area of prime concern to everyone.

3.3 Impact on National Security

In an increasingly connected world, cybercrime has gone beyond just financial gains. It can impact national security in a big way. Cybercrime is now a fully organised industry. It poses threat to national critical sectors like finance, telecom, railways, aviation, healthcare, water supply, defence, etc. Such implications also underscore the necessity for all countries to work jointly in a unified manner against cybercrime. However, strategic interests and differing priority focus areas of different countries become a huge impediment to achieve coherence in thoughts and acts. Some nations may prioritize economy and critical infrastructure, while others may be more worried about data privacy and sovereignty. The contrasting approaches on cybercrime management of western countries like the US, Canada, UK and the EU on one hand and eastern bloc countries like the Russia and China on the other, reveal differing philosophies and priorities, leading to fragmented efforts and competing approaches. The Clean-Network-Initiative of the US and the Digital-Silk-Road initiative of China represent one such conundrum in the global discourse against cybercrime. Regional Cybersecurity Agreement of the SCO represents another such regional approach. Strategic

interests of nation states are being served through cyber espionage; in such a scenario, it is detrimental to their own interests to have a strong regulatory framework which is legally binding.

3.4 Impact of New Age Technologies

Another major gap in addressing cybercrimes is ignoring the new age technology. Technologies like cloud services, IoT, digitisation of OT network, autonomous vehicles, smart homes, quantum computing, blockchain, crypto-currency frauds, digital arrest, deep fake video, audio cloning, AI enabled cybercrimes, use of TOR network, are either helping the cyber-criminals in executing more sophisticated attacks or they are providing a wider landscape for commission of cybercrime. Either way, such technologies are only contributing to the exponential rise in cybercrime. This problem needs to be tackled on two fronts; one, understanding the new forms of cybercrimes and accordingly devise anti-technology to prevent/investigate the crime; two, the legal frameworks need to be updated regularly so as not to leave any regulatory gaps that cyber-criminals can exploit.

3.5 Miscellaneous Issues

In addition to above, some other issues that need to be addressed are monitoring & ensuring policy compliances, setting up of dedicated CERTs by all nations, global shortage of cyber security professionals, inadequate training of LEA and judicial officers, need for supply chain sanitization to prevent malware, enhanced collaboration between government, industry & academia, increasing public awareness on cybercrimes and introducing cyber education at school/colleges.

4. RECOMMENDATIONS

As per the ITU GCI Report-2024, there are 105 countries that have proliferated digital services without a matching cyber security governance framework. Such a situation is very critical, as few weak spots anywhere across the globe are capable of impacting other nations, including developed ones. The recommended measures that will help to strengthen the global cybercrime governance framework, are summarised below.

Enhancing Global Cooperation. As discussed earlier, global cooperation is of utmost importance in containing the menace of trans-border cybercrime. It not only includes cooperation in investigation and adjudication of cybercrimes, but also sharing of data and threat intelligence with each other; threats building up in one geography can soon proliferate to other parts of the globe, if not addressed in time. The databases and cyber intelligence from INTERPOL and other organisations like the ENISA or the US Cybersecurity and Infrastructure Security Agency (CISA) must be made available to all state LEAs and regional bodies. Geopolitical frictions can also be resolved through dialogue and mutual cooperation; forums like the UN Open Ended Intergovernmental Experts Group can be exploited for such discussions.

Harmonizing Cyber Regulations. Cyber regulations of various countries are at variance with each other. There is difference in definitions, offences and penalties, as well as adjudication process. It is next to impossible for all countries to sit together and devise harmonised cyber laws. The only way to harmonize these aspects is for all countries to sign a common convention/treaty, like the UN Convention-2024. A prime focus area for such harmonization should be online safety of children, including protection against sexual exploitation.

Cyber Security Strategy. As per ITU, 132 nations have published their National Cyber Security Strategy, i.e. about 67.7 per cent. 63 countries have still not published a National Cyber Security Strategy. This gap needs to be covered at the earliest. International bodies like the ITU and UN must urge these countries to prepare and publish their cyber strategy.

Capacity Enhancement in Under Developed Countries. A weak framework in one country can have devastating effects in many other. It is thus our shared responsibility to not only foster an environment of mutual trust, but also help the under-developed countries in strengthening their cyber regulatory framework. It is very important there are no weak spots in the global cybercrime governance framework. Under-developed countries, who are not equipped for strengthening their cyber ecosystem need to be supported by developed nations and international organisations like Global Forum on Cyber Expertise (GFCE).

Monitoring Governance Frameworks for Effectiveness. To measure the efficacy of cybercrime governance it is required to have a set of metrics that will align with the desired end state. Reduction in cybercrimes, cyber- attacks and data breaches is a good indicator for ascertaining the efficacy of governance mechanisms. Certain countries like Singapore and Estonia have written success stories post adoption of a robust cybercrime framework. Even compliance

rates reflect the adoptability of the governance framework; for example, EU countries, after the adoption of GDPR, reported a decline in data breaches, with defaulters mainly being the non-compliant nations. As per a report, Singapore, with a compliance rate of 95 per cent had a reduction in breaches by 80 per cent, Estonia reported a 92 per cent compliance with breach reduction of 75 per cent, while EU reported a GDPR compliance of 88 per cent with reduction in breach of 70 per cent. Continuous audit of compliance also contributes towards strengthening the implementation of any convention/treaty/regulation.

Monitoring & Ensuring Compliances. Regulatory compliances are difficult to achieve; more so, for an organisation with global footprint, as it has to adhere to multiple compliances across multiple sovereign government regulatory frameworks. While penalties for non-compliance are well defined in the regulations, there are no incentives for compliance; positive regulatory compliances should be awarded through government sops like tax benefits, etc, to incentivize cyber regulatory compliances.

Dedicated CERTs. As per ITU GCI Report-2024, 139 countries have CERTs. CERTs have a critical role in keeping the track of cybercrimes, preventing cyber-attacks/breaches and provide guidance to government and industry in best safe practices. It is therefore important that all countries should set up CERTs.

Technology Update of Cyber Laws. Technology in the cyber domain is progressing very fast. It is said that technology cycle in the field of ICT is maximum 18 months. Framing and promulgation of cyber laws by any country is a very detailed, tedious and time consuming process. It is therefore not feasible to keep updating the cyber laws every time a new technology surfaces. It may be a better proposition to frame laws in a manner that they are technology agnostic and thus future-proof. To elaborate further, the act of commission should be declared a crime rather than mentioning the technology behind it; for example, today fake videos are being made using AI; apropos, it's better to state that creation and use of fake videos/voice for commission of cybercrime is an offence, instead of saying fake videos based on AI.

Availability of Cyber Security Professionals. As per a World Economic Forum (WEF) survey only 14 percent of the organisations were confident that they have adequate cyber security professionals and between 2024 and 2025, the shortage grew by eight per cent. Another report suggests that there is a 19 per cent annual increase in cyber-professionals availability gap amounting to 4.8 million unfilled positions. As per an ITU report of 2024, only 123 countries are reportedly carrying out cyber security training programs. This is a critical aspect that needs to be attended to by all. Unless the government and industry have adequately trained cyber security professionals, there will be serious security gaps in the ICT infrastructure and networks that will leave the systems vulnerable to cyber-attacks.

Training of LEA and Judicial Officers. As discussed earlier, the training of LEA and judicial officers on cybercrime issues is a must and needs dedicated efforts by all state governments. The same has also been highlighted in the UN Manual-1994 and UN Convention-2024.

Supply Chain Sanitization. As per a World Economic Forum (WEF) survey about 54 percent of the organisations reported supply chain infection as a major source of concern in regards to cyber security of their enterprise networks & IT assets. Such infections leave trap-doors in our systems that can be exploited by the cyber-criminals and even adversary nation states, to conduct cyber espionage and sabotage, both.

Collaboration Between Government, Industry and Academia. Private-Public Partnerships (PPP) are very beneficial in enhancing collaboration. This should be practiced at global as well as regional/national level. For example, the World Economic Forum Partnership Against Cybercrime, ENISA's mandate for PPP and Singapore's Cybersecurity Industry Call for Innovation, are good examples of PPP at the global & regional level. The PPP models should also include promoting cyber research and sharing of industry best practices.

Public Awareness and Education at School/Colleges. As per ITU GCI Report -2024, 152 countries are running cyber awareness campaigns for general public. It is important that others also join this initiative. In addition, introducing cyber education at school land college level will also pay handsome dividends in the long run.

Soft Mechanisms. While the global conventions, treaties and regulations play a larger formal role in fight against cybercrime, the importance of soft mechanisms cannot be undermined. These include actions like promulgation of guidelines, industry best practices, capacity enhancing, information sharing, technical assistance, public awareness, etc. While these actions may not be binding, they do support the legally binding treaties and conventions and are complimentary in efforts. The Tallinn Manual of NATO or the National Institute of Standards & Technology (NIST) Cybersecurity Framework of US are good examples of such soft measures.

Process Workflow for Investigation of a Trans-Border Cybercrime. Based on the discussion above and the unique complexities involved in a cybercrime, a suggested process workflow for investigation and adjudication of a trans-border cybercrime is as given below:

- Step 1. Cybercrime or cyber-attack is reported by the victim or system/personal alerts. These should be reported to the relevant government agency, as per the gravity of crime. Further, a quick analysis should be done to assess the extent of damage, source of crime and its global footprint.
- Step 2. Based on the global footprint of accused, victim, route trace and deposition of crime proceeds, the territorial jurisdiction needs to be decided. This is followed by an assessment of regulatory frameworks of the jurisdictions involved and accordingly, selection of the cooperation mechanism.
- Step 3. The immediate requirement should be to secure the electronic evidence, as its shelf life is low and it is prone to tampering easily and quickly. This is followed by evidence collection and forensic analysis.
- Step 4. This stage involves engaging with global agencies like INTERPOL and exploiting existing treaties/conventions like Budapest Convention-2001, UN Convention-2024, mutual legal assistance, etc for cooperation. Documentation should be prepared for legal proceedings.
- Step 5. This is the last stage in which a review of the whole process should be done with a view to learn for future.

5. CONCLUSION

Mitigation of cybercrime through global treaties needs a coordinated and unified approach. The increasing use of new age technologies by cyber-criminals necessitates a legally binding framework that transcends geographical boundaries. Keeping our individual aspirations aside, all countries need to work towards the single aim of preventing and curbing cybercrime in all forms. Global regulations provide accountability amongst sovereign governments and private entities, both. Organisations like the ITU, UN, EU, AU, etc should to continue to provide common platforms for engagements by all stakeholders and build trust based relationships in addition to the legally binding regulations. In addition, capacity building in developing countries will also help in making the framework more resilient and agile. A combined approach, comprising of legal, technical, policy and cooperation measures will help the global society to put up a strong fight against cybercrime. Nations need to work together, in unison, to achieve this.

Global regulations play a major role in containing cybercrime and ensuring effective investigation and adjudication. However, their impact and efficiency is dependent on achieving consensus and common grounds of understanding the law and investigation mechanisms. Various world bodies have contributed to management of this menace, like the CoE's Budapest Convention-2001, the SCO Agreement, the UN Convention-2024, INTERPOL and NATO initiatives, etc. A combine and unified approach to tackling this menace is the only way ahead. Differing interpretations and multiple legal frameworks will always keep hindering the progress in this domain. It is therefore of utmost importance that a harmonised approach is adopted by all, not only in following legally binding conventions but also in developing mutual trust and collaborative mindset. It is also critical that all such global agreements keep getting revised in tune with the advent of new technologies and new methods being employed by the cyber-criminals.

References

1. African Union (AU). 2014. *The African Union (AU) Convention on Cyber Security and Personal Data Protection (Malabo Convention)*. Available at https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf. Retrieved 25 Dec 2025.
2. Ahmed, Tamzid. 06 May 2026. 256 *Cybercrime Statistics for 2025*. Brightdefense.com. Available at https://www.brightdefense.com/resources/cybercrime-statistics/. Retrieved 04 Jul 2026.
3. Bogdanoski, Mitko and Petreski, Drage. Jul 2013. *Cyber Terrorism– Global Security Threat*. International Scientific Defence, Security and Peace Journal. pp. 59-72. Available at https://www.researchgate.net/profile/Mitko-Bogdanoski/publication/252195165_CYBER_TERRORISM-_GLOBAL_SECURITY_THREAT/links/02e7e51f2935a238da000000/CYBER-TERRORISM-GLOBAL-SECURITY-THREAT.pdf?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6Il9kaXJlY3QiLCJwYWdlIjoicHVibGljYXRpb24iLCJwcmV2aW91c1BhZ2UiOiJfZGlyZWN0In19. Retrieved 03 Jul 2026.
4. Brightdefense. Jun 2025. *Cybercrime Statistics for 2025*. Available at https://www.brightdefense.com/resources/cybercrime-statistics/. Retrieved 04 Jul 2026.

5. Bruce, M., Lusthaus, J., Kashyap, R., Phair, N. and Varese, F. 10 Apr 2024. *Mapping the global geography of cybercrime with the World Cybercrime Index*. PLOS One. Available at https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0297312&utm_referrer=https%3A%2F%2Fdzen.ru%2Fmedia%2Fid%2F62e6d9ea417ab83ed9b24daa%2F66cc1ab6c4f43a1b1a5f3314. Retrieved 31 Dec 2025.
6. Buçaja, Enver and Idrizaj, Kenan. 19 Sep 2024. *The need for cybercrime regulation on a global scale by the international law and cyber convention.* Multidisciplinary Reviews: Malque Publishing. Available at https://www.malque.pub/ojs/index.php/mr/article/view/5348/2474. Retrieved 05 Jun 2026.
7. Chauhan, Ashish. Mar 2025. *Hacking as a service sells in dark web for just Rs 38k*. The Times of India.
8. Cooperative Cyber Defence Centre of Excellence (CCD-CoE). n.d. Available at https://ccdcoe.org/about-us/. Retrieved 05 Feb 2026.
9. Cooperative Cyber Defence Centre of Excellence (CCD-CoE). n.d. *International Conference on Cyber Conflict – CyCon.* Available at https://ccdcoe.org/cycon/. Retrieved 01 Jul 2026.
10. Cooperative Cyber Defence Centre of Excellence (CCD-CoE). n.d. *The Tallinn Manual.* Available at https://ccdcoe.org/research/tallinn-manual/. Retrieved 30 Jun 2026.
11. Council of Europe (CoE). 12 May 2022. *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224)*. Available at https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=224. Retrieved 30 Jun 2026.
12. Council of Europe (CoE). 1995. *CoE Recommendation No R(95)13*. Available at https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804f6e76. Retrieved 25 Dec 2025.
13. Council of Europe (CoE). 23 Nov 2001. *Convention on Cybercrime (Budapest)*. Available at https://rm.coe.int/1680081561. Retrieved 05 Jan 2026.
14. Council of Europe (CoE). 28 Jan 2003. *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189)*. Available at https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=189. Retrieved 30 Jun 2026.
15. Council of Europe (CoE). n.d. *The Convention on Cybercrime (Budapest Convention, ETS No. 185) and its Protocols.* Available at https://www.coe.int/en/web/cybercrime/the-budapest-convention. Retrieved 17 Jun 2026.
16. Council of Europe. 1989. *Recommendation 89(9) on Computer Related Crime.* Available at https://www.oas.org/juridico/english/89-9&final%20Report.pdf. Retrieved 04 Dec 2025.
17. Cyble. Jul 2025. *Executive Report on the Cyber Conflict: Iran-Israel*. Available at https://cyble.com/. Retrieved 31 Dec 2025.
18. EU Agency for Cybersecurity (ENISA). 2025. *The European Union Agency for Cybersecurity. Towards a Trusted and Cyber Secure Europe.* Available at https://www.enisa.europa.eu/about-enisa/who-we-are. Retrieved 08 May 2026.
19. European Commission. 06 Mar 2025. *Cyber Resilience Act.* Available at https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act. Retrieved 25 Apr 2026.
20. European Commission. 07 Nov 2024. *Protecting children from sexual abuse*. Available at https://home-affairs.ec.europa.eu/policies/internal-security/protecting-children-sexual-abuse_en. Retrieved 25 Apr 2026.
21. European Commission. 15 Sep 2022. *Regulation of The European Parliament and of The Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020*. Available at https://eur-lex.europa.eu/resource.html?uri=cellar:864f472b-34e9-11ed-9c68 01aa75ed71a1.0001.02 /DOC_1&format=PDF. Retrieved 25 Apr 2026.
22. European Commission. 17 Jan 2025. *Digital Operational Resilience Act (DORA).* Available at https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en. Retrieved 25 Jun 2026.
23. European Commission. 2022. *We Protect Global Alliance to end child sexual exploitation online*. Available at https://home-affairs.ec.europa.eu/policies/internal-security/protecting-children-sexual-abuse/cooperation-against-child-sexual-abuse/we-protect-global-alliance-end-child-sexual-exploitation-online_en. Retrieved 19 Jun 2026.
24. European Union (EU). 2018. *General Data Protection Regulation*. Available at https://gdpr-info.eu/. Retrieved 26 Dec 2025.
25. Europol. n.d. *European Cybercrime Centre EC3*. Europol. Available at https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3. Retrieved 02 Jun 2026.
26. Federal Bureau of Investigation (FBI), Government of USA. n.d. *Most Wanted, Evgeniy Mikhailovich Bogachev*. Available at https://www.fbi.gov/wanted/cyber/evgeniy-mikhailovich- Bogachev. Retrieved 07 Jun 2026.
27. Gakiria, Andrew and Gitonga, Tevin Mwenda. 29 Jan 2025. *What is the Malabo convention?* Diplomacy.Edu. Available at https://www.diplomacy.edu/blog/what-is-the-malabo-convention/. Retrieved 02 Jan 2026.
28. Georgetown Law. 17 Mar 2025. *International and Foreign Cyberspace Law Research Guide: IGO, NGO, & U.S. Government Agency Resources*. Available at https://guides.ll.georgetown.edu/cyberspace/cyber-crime-igos-and-ngos. Retrieved 06 Jul 2026.
29. International Criminal Police Organisation (INTERPOL). 30 Nov 2016. *Avalanche Network Dismantled in International Cyber Operation*. Available at https://www.interpol.int/ar/1/1/2016/Avalanche-network-dismantled-in-international-cyber-operation. Retrieved 04 Jul 2026.

30. International Criminal Police Organisation (INTERPOL). Apr 2021. *INTERPOL National Cybercrime Strategy Guidebook*. p. 3. Available at https://www.interpol.int/content/download/16455/file/Cyber%20Strategy%20Guidebook.pdf. Retrieved 02 Jul 2026.
31. International Criminal Police Organisation (INTERPOL). n.d. *Completed ICT Law Projects*. Available at https://www.interpol.int/Who-we-are/Legal-framework/Information-communications-and-technology-ICT-law-projects/Completed-ICT-law-projects. Retrieved 30 Jun 2026.
32. International Criminal Police Organisation (INTERPOL). n.d. *Cyber Capabilities Capacity Development Project*. Available at https://www.interpol.int/Crimes/Cybercrime/Cyber-capabilities-development/Cyber-Capabilities-Capacity-Development-Project. Retrieved 30 Jun 2026.
33. International Criminal Police Organisation (INTERPOL). n.d. *Cybercrime Collaboration Services*. Available at https://www.interpol.int/Crimes/Cybercrime/Cybercrime-Collaboration-Services. Retrieved 30 Jun 2026.
34. International Criminal Police Organisation (INTERPOL). n.d. *Cybercrime Threat Response*. Available at https://www.interpol.int/Crimes/Cybercrime/Cybercrime-threat-response. Retrieved 30 Jun 2026.
35. International Criminal Police Organisation (INTERPOL). n.d. *EVIDENCE2e CODEX*. Available at https://www.interpol.int/Who-we-are/Legal-framework/Information-communications-and-technology-ICT-law-projects/EVIDENCE2e-CODEX. Retrieved 30 Jun 2026.
36. International Criminal Police Organisation (INTERPOL). n.d. *Our 19 Databases*. Available at https://www.interpol.int/How-we-work/Databases/Our-19-databases. Retrieved 30 Jun 2026.
37. International Criminal Police Organisation (INTERPOL). n.d. *Project Titanium*. Available at https://www.interpol.int/Who-we-are/Legal-framework/Information-communications-and-technology-ICT-law-projects/Project-Titanium. Retrieved 30 Jun 2026.
38. International Criminal Police Organisation (INTERPOL). n.d. *Public Private Partnerships*. Available at https://www.interpol.int/Crimes/Cybercrime/Public-private-partnerships. Retrieved 30 Jun 2026.
39. International Criminal Police Organisation (INTERPOL). n.d. *Speaker Identification Integrated Project (SIIP).* Available at https://www.interpol.int/Who-we-are/Legal-framework/Information-communications-and-technology-ICT-law-projects/Speaker-Identification-Integrated-Project-SIIP. Retrieved 30 Jun 2026.
40. International Criminal Police Organisation (INTERPOL). n.d. *What is INTERPOL?* Available at https://www.interpol.int/Who-we-are/What-is-INTERPOL2. Retrieved 29 Jun 2026.
41. International Telecommunication Union (ITU). 12 Sep 2024. *Countries strengthening cybersecurity efforts, but increased action still required: UN cybersecurity report assesses global progress in providing a safe and secure digital future for all*. Available at https://www.itu.int/en/mediacentre/Pages/PR-2024-09-10-Global-Cybersecurity-Index.aspx. Retrieved 04 Jul 2026.
42. International Telecommunication Union (ITU). 2007. Available at https://www.itu.int/en/action/cybersecurity/pages/gca.aspx. Retrieved 25 Jun 2026.
43. International Telecommunication Union (ITU). 2024. *Global Cybersecurity Index*. https://www.itu.int/en/ITU-D/Cybersecurity/pages/global-cybersecurity-index.aspx, Retrieved 28 Jun 2026.
44. KonBriefing. Jun 2025. *Cyber-attack news today 2025*. Available at https://konbriefing.com/en-topics/cyber-attacks.html. Retrieved 24 Jun 2026.
45. Luthi, Ben. 30 Jun 2025. *Here's What Your Data Sells for on the Dark Web*. Available at https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/. Retrieved 02 Jul 2026.
46. Mali, Prashant. Dec 2024. *International Cybercrime Treaties and Case Laws: An Overview*. Cyber Law Consulting. Available at https://www.cyberlawconsulting.com/global_cybersecurity_sco_framework.php. Retrieved 02 Jan 2026.
47. Mallick, Maj Gen P K, (Retired). Jul 2024. *Protection of Critical Information Infrastructure*. p 23. Vivekananda International Foundation. Available at https://www.vifindia.org/sites/default/files/Protection-of-Critical-Information-Infrastructure.pdf. Retrieved 25 May 2026.
48. Naseeb, Shujaat and Khan, Wajahat Naseeb. 2024. *Mitigating Cybercrime through International Law: The Role of Global Cybersecurity Agreements.* Mayo RC Journal of Communication for Sustainable World. 1(1). p 31-40. Available at https://www.researchcorridor.org/index.php/mcj/article/view/145/135. Retrieved 25 Apr 2026.
49. National Health Service (NHS), Government of UK. 2023. *NHS England Business Continuity Management Toolkit Case Study: WannaCry Attack*. Available at https://www.england.nhs.uk/long-read/case-study-wannacry-attack/. Retrieved 04 Jul 2026.
50. NATO. n.d. *The Tallinn Manual*. Available at https://ccdcoe.org/research/tallinn-manual/. Retrieved 26 Dec 2025.
51. NDTV.Com. 23 Jun 2026. *Apple, Tesla Secrets Leaked in Tata Electronics Cyber breach? What We Know*. Available at https://www.ndtv.com/business-news/tata-electronics-cyberbreach-apple-tesla-trade-secrets-cybersecurity-china-11675458. Retrieved 29 Jun 2026.
52. Nigam, Nidhi. 30 Nov 2024. *The Role of Artificial Intelligence and Machine Learning in Enhancing Cybersecurity against Cybercrime*. ECCouncil. Available at https://www.eccouncil.org/cybersecurity-exchange/network-security/role-of-ai-ml-in-enhancing-cybersecurity-against-threats/. Retrieved 25 Jan 2026.
53. North Atlantic Treaty Organisation (NATO). 2013. *Tallinn Manual on The International Law Applicable to Cyber Warfare*. Available at http://csef.ru/media/articles/3990/3990.pdf. Retrieved 25 Dec 2025.

54. Osborne, Charlie. 2025. *Satan ransomware-as-a-service starts trading in the Dark Web*. ZDNET. Available at https://www.zdnet.com/article/satan-ransomware-as-a-service-starts-trading-in-the-dark-web/. Retrieved 22 Feb 2026.
55. Perlroth, Nicole. 03 Oct 2017. *All 3 Billion Yahoo Accounts Were Affected by 2013 Attack*. The New York Times. Available at https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html. Retrieved 30 Jun 2026.
56. Programs. Com. n.d. Available at https://programs.com/resources/cybercrime-cost/. Retrieved 05 Jul 2026
57. Qudus, Lawal. 21 Jan 2025. *Cybersecurity governance: Strengthening policy frameworks to address global cybercrime and data privacy challenges*. International Journal of Science and Research Archive. 14(01). pp. 1146-1163. Available at https://journalijsra.com/sites/default/files/fulltext_pdf/IJSRA-2025-0225.pdf, Retrieved 16 Jun 2026.
58. Race Labs. 18 Feb 2026. *Biggest Cyber Attacks of 2026 & Their Impact on Global Cybersecurity*. Available at https://race.reva.edu.in/race-lab/biggest-cyber-attacks-of-2026. Retrieved 24 Jun 2026.
59. Schjolberg, Stein. Dec 2008. *The History of Global Harmonization on Cybercrime Legislation - The Road to Geneva*. p. 4. Cybercrimelaw. Available at https://cybercrimelaw.net/documents/cybercrime_history.pdf. Retrieved 04 Apr 2026.
60. Singh, Tripti. Sep 2024. *Cybercrime and International Law: Jurisdictional Challenges and Enforcement Mechanisms.* African Journal of Biomedical Research 27(3). 697-708. Available at https://africanjournalofbiomedicalresearch.com/index.php/AJBR/ article/download/2101/1829/3822. Retrieved 30 Jun 2026.
61. Tafazzoli, Tala. 2018. *Cybercrime Legislation*. International Telecommunication Union (ITU). Available at https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/SiteAssets/Pages/Events/2018/Cyber securityASPCOE/cyber security/Tafazzoli-cybercrime%20legislations.pdf. Retrieved 26 Dec 2025.
62. The Indian Express. 07 May 2026. *Thwarted 68 lakh cyber attacks on ECINET portal on counting day: Election Commission*. Available at https://indianexpress.com/article/india/ecinet-portal-cyberattack-election-commission-68-lakhmalicious-hits-2026-results-10676447/. Retrieved 02 Jul 2026.
63. The Shanghai Cooperation Organisation (SCO). (2017, January 9). *General Information: Cooperation with International and Regional Organizations.* Available at https://eng.sectsco.org/20170109/192193.html. Retrieved 30 Jun 2026.
64. The Shanghai Cooperation Organisation (SCO).16 Jun 2009. *Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization*. p. 3,4, 11-13. Available at https://eng.sectsco.org/files/207508/207508. Retrieved 30 Jun 2026.
65. UN Office on Drugs and Crime (UNODC). Feb 2013. *Comprehensive Study on Cybercrime: February 2013*. p. 183-184. Available at https://www.unodc.org/documents/organised-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf. Retrieved 24 May 2026.
66. UN Office on Drugs and Crime (UNODC). n.d. *UNODC: Our Mandate*. Available at https://www.unodc.org/unodc/en/cybercrime/our-mandate. Retrieved 24 May 2026.
67. UN Office on Drugs and Crime (UNODC). n.d. *UNODC: Who We Are and What We Do*. Available at https://www.unodc.org/documents/Advocacy-Section/UNODC-at-a-glance_PRINT.pdf. Retrieved 24 Jun 2026.
68. United Nations (UN). 13 Jan 2015. *Developments in the field of information and telecommunications in the context of international security*. Available at https://digitallibrary.un.org/record/786846/files/A_69_723-EN.pdf. Retrieved 25 Jun 2026.
69. United Nations (UN). 19 Apr 2021. *Report on the meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime held in Vienna from 6 to 8 April 2021*.Available at https://documents.un.org/doc/undoc/gen/v21/025/95/pdf/v2102595.pdf?OpenElement. Retrieved 26 Dec 2025.
70. United Nations (UN). 24 Dec 2024. *United Nations Convention Against Cybercrime-2024*. pp. 5-8, 24-37, 44-46. Available at https://documents.un.org/doc/undoc/gen/n24/372/04/pdf/n2437204.pdf. Retrieved 02 Jul 2026.
71. United Nations Office on Drugs and Crime (UNODC). 1994. *UN Manual on Prevention and Control of Computer Related Crime.* Available at https://www.unodc.org/pdf/Manual_ComputerRelatedCrime.PDF. Retrieved 30 Nov 2025.
72. United Nations Office on Drugs and Crime (UNODC). n.d. *UNODC Global program on Cybercrime*. https://www.unodc.org/unodc/en/cybercrime/index.html. Retrieved 28 May 2026.
73. United Nations. 24 Dec 2024. *UN General Assembly adopts landmark convention on cybercrime*. Available at https://www.unodc.org/unodc/en/press/releases/2024/December/un-general-assembly-adopts-landmark-convention-on-cybercrime.html. Retrieved 25 Apr 2026.
74. Uzor, Diana. 31 Oct 2025. *21 African Countries Sign UN Cybercrime Convention, Ghana Calls for Input on 14 Digital Bills, and South Africa's AI Policy progresses*. Available at https://www.linkedin.com/pulse/21-african-countries-sign-un-cybercrime-convention-ghana-diana-uzor-qtqcf/. Retrieved 02 Jul 2026.
75. Verma, Anoop. 07 Mar 2023. *India's dream of USD 5 trillion economy threatened by cybercrime risks*. The Economic Times. Available at https://government.economictimes.indiatimes.com/news/secure-india/indias-dream-of-usd-5-trillion-economy-threatened-by-cybercrime-risks-are-the-systems-in-place-to-tackle-it/98464431. Retrieved 25 Dec 2025.
76. World Economic Forum (WEF). Jan 2025. *Global Cybersecurity Outlook 2025*. Available at https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf. Retrieved 04 Jul 2026.