

Cyber Terrorism: International Legal Regulations And Efforts

Paper Id : **21066** Submission Date : **2026-01-03** Acceptance Date : **2026-01-11** Publication Date : **2026-01-13**

This is an open-access research paper/article distributed under the terms of the Creative Commons Attribution 4.0 International, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

DOI:10.5281/zenodo.18277455

For verification of this paper, please visit on <http://www.socialresearchfoundation.com/innovation.php#8>



Shelly Aggarwal

Research Scholar
Department Of Laws
Panjab University
ChandigarhIndia

Abstract

Cyberterrorism, a transnational issue, requires effective international and regional laws. Initiatives like the Budapest Convention on Cybercrime, UNODC Global Program on Cybercrime, and UNSC Resolutions (1373, 57/239, 1624, and 2462) aim to address this global problem. However, challenges persist due to divergent national laws, jurisdictional complexities, and time-sensitive digital evidence. Effective cooperation requires accelerated data preservation, 24/7 points of contact, and specialized tools. As AI and quantum technologies evolve, so do threats, necessitating concerted responses, multilateral coordination, and technological resilience investments to counteract cyber threats to critical information infrastructure all while balancing law enforcement with human rights and sovereignty concerns.

Keywords

Cyber Terrorism, International Laws, Technology, Multilateral Coordination, Critical Information Infrastructure.

Introduction

Cyber terrorism is a serious 21st-century security concern, blurring lines between warfare and crime. Unlike traditional terrorism, it leverages digital infrastructure to attack vital services and spread terror globally. This requires strong international frameworks, collective policies, and combined efforts.

At the international level, the United Nations has taken substantial steps, particularly through Security Council Resolution 1373, which focuses on limiting terrorist financing, while the International Telecommunication Union (ITU) advances cybersecurity standards. The Council of Europe's Budapest Convention on Cybercrime harmonizes laws, but a binding treaty on cyber terrorism remains elusive.[1].

Divergent national laws, jurisdictional overlaps, and sovereignty concerns hinder a unified global strategy. Technology also outpaces legal frameworks, creating loopholes. A balanced strategy protecting security while preserving basic rights is crucial for effective action against cyber terrorism[2].

Objective of study

This paper aims to explore the international legal framework addressing the spread of cyberterrorism vis-à-vis technological advancement challenges in past few decades.

Review of Literature

This paper is based on various books and literature which are discussed through out the paper.

Main Text

1.2 Cyber Terrorism and Global Concerns

Cyberterrorism is a 21st-century security threat where terrorism meets cyberspace. The FBI defines it as planned, politically motivated cyberattacks by subnational actors, distinct from regular cybercrime. Dorothy Denning broadens this to include attacks meant to intimidate or coerce governments/societies for political/social goals, causing violence or fear. It involves non-state actors using cyber capabilities to interfere with populations, governments, or organizations on a large scale, aiming to create terror, destabilize nations, and sow fear for political/ideological motives.

Cyber-attacks like malware, phishing, and ransomware disrupt critical infrastructure, causing physical, social, and economic damage[3]. These attacks can cascade, leading to mass blackouts, transport delays, and financial losses that destabilize regions. The 2017 WannaCry attack hit 150 nations, inflicting billions in damages.

Cyberterrorism affects national economies through direct losses, reduced productivity, stolen IP, and reputational damage. Stolen intellectual property and trade secrets can compromise a nation's competitiveness in the global marketplace, while reputational damage internationally can influence foreign capital inflows and tourism[4].

The psychological aspect is significant, with cyberspace offering deniability and anonymity for hostile activities. Unchecked, cyber-attacks may spiral into cyber warfare, disturbing global peace and security. The absence of clear attribution procedures makes it even more difficult to respond diplomatically to such attacks, fostering an atmosphere of suspicion and distrust between nations[5].

The Solar Winds 2020 attack targeted government agencies and private institutions, showing advanced actors can breach key systems and potentially undermine national security. Attacks on electoral systems raise concerns about democratic institutions' integrity and the possibility of cyberterrorism affecting political processes[6].

Cyberterrorism threatens global peace, security, and economic stability, risking diplomatic breakdowns and tensions. As a transnational issue, it requires robust international law frameworks. The Budapest Convention on Cybercrime (80+ nations) harmonizes cybercrime laws and cooperation but focuses more on cybercrime than cyberterrorism. To fill this gap, the UN is working on a comprehensive Convention against Cybercrime, and the UNODC Global Programme on Cybercrime assists states with capacity building, training and rapid response instruments[7]. Strengthened legal regimes, international cooperation, and capacity-building are crucial to counter cyberterrorism and protect global security and democratic institutions [8].

1.3 Council of Europe and the Convention on Cybercrime (2001)

The Council of Europe played a pioneering role in addressing cybercrime challenges in the 21st century. Recognizing the transnational nature of digital offenses, it adopted the Convention on Cybercrime (2001), aka the Budapest Convention, to harmonize national legal responses and enable international cooperation against cybercrimes. As the first international treaty on internet/computer network crimes, it remains a cornerstone of global cyber law frameworks. Open to non-European states, it's gained almost universal reach[9].

Key Provisions of the Budapest Convention

The Budapest Convention tackles cybercrime by introducing substantive and procedural provisions. Substantive provisions define offenses like breaches of computer system/data confidentiality, integrity, and availability, computer-related offenses, content-related offenses and copyright/IPR infringements[10]. Procedural provisions enable investigations with measures like expedited preservation of stored data, real time collection of traffic data and content interception and production orders and search/seizure of data for enabling investigators to lawfully obtain necessary evidence[11]. The Convention's framework for cross-border cooperation is key, with obligations for states to assist in investigations and prosecutions through mutual legal assistance, extradition, and a 24/7 contact network for rapid response. In doing so, it anticipates the jurisdictional complexities inherent to cybercrime, where perpetrators, victims, and servers may all be located in different countries.

Protocols Addressing Xenophobia and Racism Online

The Council of Europe adopted an Additional Protocol to the Convention on Cybercrime (2003) to tackle hate speech, xenophobia, and extremist propaganda online. It requires signatories to criminalize dissemination of racist/xenophobic material, threats motivated by racial/religious hatred and denial/justification of genocide or crimes[12].

This helps prevent online spaces becoming havens for intolerance and racial hatred[13] and addresses the ideological roots of terrorist violence, as extremist groups exploit online platforms for hate, recruitment, and radicalization. By criminalizing xenophobic and racist propaganda online, the Protocol strengthens the capacity of states to address the ideological underpinnings of terrorist violence[14].

Relevance for Cyber Terrorism Investigations and Extradition

The Budapest Convention and its Protocols have substantial relevance for contemporary challenges posed by cyber terrorism. The Convention tackles cyber terrorism challenges through harmonization and cooperation in following ways:

1. Facilitating swift and technologically relevant investigations with real-time interception, data preservation, and access to stored data indispensable in tracing cyber terrorists who rely on encryption, anonymity tools, and rapidly disappearing digital footprints.
2. Cross-border evidence gathering by sharing data stored on servers across multiple jurisdictions. The states are obligated to cooperate in preserving and sharing such data, thereby bridging jurisdictional gaps. It allows securing of crucial evidence without being hampered by fragmented domestic laws[15].
3. Extradition provisions to prevent safe havens for terrorists
4. Preventing abuse of cyberspace for terrorism by criminalizing hate speech and propaganda, it disrupts the communication channels used by terrorist organizations

to mobilize support.

5. Global relevance with adoption by countries worldwide, enhancing effectiveness against borderless cyber threats[16].

The Council of Europe's Convention on Cybercrime (2001) and its subsequent Protocols represent foundational instruments in the international community's effort to regulate cyberspace. By introducing substantive criminal provisions, equipping authorities with procedural powers, and ensuring mechanisms for international cooperation, the Budapest Convention created a model legal framework that continues to guide global responses to cybercrime and cyber terrorism alike. The Protocol addressing xenophobia and racism online further illustrates the Council of Europe's foresight in confronting the misuse of digital platforms for extremist purposes. In the context of cyber terrorism, these instruments remain vital in ensuring that the digital realm does not become a lawless arena for transnational threats, but rather a regulated space where states can collectively safeguard security, human dignity, and the rule of law.

1.4 Role of the United Nations in Combating Cyber Terrorism

The UN plays a key role in coordinating global action against cyber terrorism through security Council resolutions, strategic programs targeting digital threats, multi-dimensional approach including legal frameworks, capacity development and international cooperation mechanisms aimed at combating terrorist abuse of information and communications technology (ICT)[17].

(i) UNSC Resolution 1373 (2001) and Counter-Terrorism Committee

Security Council Resolution 1373, adopted on September 28, 2001, in response to the September 11 terrorist attacks, created the underlying architecture for international action against terrorism and established the Counter-Terrorism Committee (CTC). The resolution calls on all Member States to take robust steps to prevent financing, planning, providing support, or committing terrorist acts, including terrorist acts using cyber technologies. The resolution directly urges Member States to seek ways to increase and speed up the exchange of operational information regarding the use of ICT by terrorist groups and to counter terrorist recruitment[18].

(ii) Resolution 1624 (2005) and Reinforcing Counter-Terrorism Steps

Security Council Resolution 1624 (2005) tackles incitement to terrorism, including through online means in following ways:

1. Urges states to ban incitement to commit terrorist acts
2. Addresses terrorist use of internet and social media for radicalization and recruitment
3. Emphasizes balancing security with human rights, especially freedom of expression
4. Calls for counter-narrative strategies against online terrorist propaganda
5. Requires states to ensure compliance with international law, including human rights law.

This involves creating legal frameworks to criminalize incitement online while guaranteeing proper guarantees to protect legitimate expression and prohibiting the abuse of counter-terrorism legislation to stifle dissent[19].

(iii) UN Global Counter-Terrorism Strategy and Its Cyber Dimensions

The UN Global Counter-Terrorism Strategy (2006) is a comprehensive framework addressing cyber terrorism through four pillars: [20]

1. Pillar I: Eliminate online radicalization
2. Pillar II: Prevent threats via international cooperation and cybersecurity capacity building
3. Pillar III: Enhance states' counter-terrorism capacity with UN support
4. Pillar IV: Uphold human rights and rule of law in counter-terrorism efforts

Recent focus areas include:

1. Critical infrastructure threats
2. Virtual asset abuse
3. AI's dual use in terrorism/counter-terrorism
4. The threats arising from new financial technologies and virtual payment systems in financing terrorism (Resolution 2462, 2019).[21]

1.5 United Nations Resolutions and Conventions on International Security

The UN has taken steps to tackle global threats like terror, cyber insecurity, and maritime threats. Three key tools that represent the UN's positive action to enhance international security architecture[22] are:

(i) **Resolution 57/239 (2002)**: Promotes a global culture of cybersecurity, focusing on awareness, policy-building, and tech and knowledge transfer to developing nations to improve their cybersecurity capabilities.[23]. The resolution emphasizes capacity building, sharing of information, and collaboration between member states to address increasing cyber threats.

(ii) **UN Convention on Safety of Protected Persons (1973)**: Protects diplomats, heads of state, and officials from attacks and kidnappings. This treaty arose as a result of growing cases of kidnapping, murder, and attacks directed at internationally protected persons in the 1960s and the early 1970s.[24].

(iii) **Maritime Terrorism Conventions (1988)**: The seas have always been central to global commerce, communication, and strategic security. To counter the emergence of maritime terrorism, piracy, and illegal use of marine resources in late 20th century two significant conventions that were adopted in 1988 are worth mentioning[25]:

1. **SUA Convention**: Prevents maritime terrorism, piracy, and illegal acts threatening maritime security. It provides clarity on jurisdiction and extradition of offenders for prosecution and supports international cooperation by mandating the exchange of information, investigation assistance, and coordination of naval measures to enforce strengthen regional maritime security[26].
2. **Continental Shelf Protocol**: Secures offshore installations like oil rigs, gas installations and underwater structures against terrorism and sabotage. The Protocol criminalizes forcible control of a fixed platform, violent acts that put individuals on platforms in danger and leaving destructive devices on installations.

Combined together these both instruments have established a strong structure against maritime terrorism in order to maintain the security of international shipping lines and offshore resources[25]. Their relevance has only increased in the 21st century, as piracy off Somalia's coast, the vulnerability of South China Sea shipping routes, and dangers to offshore oil installations in the Middle East have all increased.

1.6 Aviation and Transport Security Conventions Relevant to Cyber Terrorism

The international aviation and transport security law has historically evolved in response to acts such as hijacking, sabotage, and bombings. It demonstrates a continuing concern with safeguarding civil aviation against unlawful interference. The advent of cyber terrorism has broadened the spectrum of threats to aviation and transport infrastructure. Modern systems rely extensively on digital technologies, satellite communications, and networked operations, making them vulnerable to malicious cyber intrusions.

The principles underlying Tokyo (1963), Hague (1970), and Montreal (1971) originally tailored to physical acts of aviation sabotage, are now being extended to address digital threats. Collectively, these conventions embody key legal principles: international cooperation, universality of jurisdiction, deterrence through criminalization, and the extension of protection beyond passengers to aviation infrastructure. Although crafted in an era of physical threats, these principles remain directly relevant in responding to the modern challenge of cyber terrorism[28]. Furthermore, the International Civil Aviation Organization (ICAO) has taken a leadership role in this transformation, particularly through its 2019 cybersecurity strategy[29].

Extension of Principles to Digital Threats to Aviation Systems

As aviation entered the digital age, its reliance on interconnected networks, air traffic management systems, and satellite navigation exposed new vulnerabilities. The potential threats are in the form of hacking air traffic control software to compromising communication between pilots and ground staff, spoofing GPS signals, or manipulating airline operational databases[30]. In this context, the core legal concepts of the earlier conventions find contemporary relevance:

1. **Jurisdiction and Accountability**: Cyber terrorists targeting aviation systems should face universal jurisdiction, like hijackers under the Hague Convention.
2. **Protection of Infrastructure**: Digital systems like air traffic management software, communication satellites and airline operational platforms are protected under the Montreal Convention's precedent.
3. **International Cooperation**: States must share info, investigate jointly, and harmonize cyber defense protocols, as per the Tokyo Convention.
4. **Deterrence through Criminalization**: Cyber intrusions into aviation systems should be criminalized, following the model of hijacking and sabotage conventions, whether or not they cause immediate physical harm.

Thus, while the conventions themselves may not explicitly mention digital threats, their principles provide a strong normative foundation for adapting legal frameworks to the cyber era. The extension of these doctrines underscores the continuity of international aviation law in addressing emerging threats[31].

ICAO Cybersecurity Strategy (2019)

Recognizing the urgency of cyber threats, the International Civil Aviation Organization (ICAO) adopted a comprehensive cybersecurity strategy in 2019. This marked a watershed in integrating cyber resilience into global aviation security governance. The strategy is premised on the idea that cybersecurity in aviation is not merely a technical challenge but a matter of international law, cooperation, and governance. The strategy emphasizes:

1. the development of resilient aviation systems capable of anticipating, withstanding, and recovering from cyberattacks. It encourages states to integrate cybersecurity into safety management systems.
2. harmonized regulations and practices across member states thus aligning national laws with international norms, fostering trust, and creating a culture of mutual assistance in cybersecurity matters.
3. the need to strengthen human and institutional capacity, particularly in developing countries, to ensure that cyber defenses in aviation are globally consistent. Training, knowledge-sharing, and technical assistance are integral to this effort.
4. promotion of secure platforms for sharing cyber threat intelligence among states, airlines, airports, and technology providers ensuring early detection and coordinated response to threats[32].
5. embedding cybersecurity into ICAO's broader aviation governance system, ensuring that states are accountable for compliance and reporting.
6. It also encourages the private sector's involvement, recognizing its crucial role in providing aviation technology and infrastructure.

By adopting this strategy, ICAO effectively bridges the gap between traditional aviation conventions and the modern cyber threat landscape. It represents a proactive, forward-looking approach, ensuring that the foundational principles of aviation security evolve with technological advancements. Together, the older instruments and the ICAO strategy highlight the adaptability of international aviation law, ensuring that the skies remain secure in both physical and digital domains[33].

1.7 International Telecommunication Union (ITU) Initiatives

The International Telecommunication Union (ITU), one of the specialized United Nations agencies, has a pivotal function in the development, regulation, and standardization of global information and communication technologies (ICT) enabling global connectivity and secure communication infrastructure. Its actions aim at closing the digital gap, administering spectrum resources, and improving cybersecurity globally[34].

Global Cybersecurity Agenda (2007): In 2007, ITU introduced Global Cybersecurity Agenda (GCA), a milestone effort to enhance cybersecurity around the globe by promoting international cooperation and capacity building. The GCA is anchored on five indispensable pillars: legal measures, technical and procedural measures, organizational structures, capacity building, and international cooperation. The broad framework helps nations develop national cybersecurity policies and strategies responding to new challenges such as cybercrime, espionage, and attacks on infrastructure [35].

Collaboration with Member States for Cyber Resilience: ITU actively supports telecommunication resilience through collaborative actions with member states, regional organizations, private sector partners, academia and industry, prioritizing emergency communications, disaster response, and protection of critical infrastructure. The organization facilitates forums for discussion on policy making, capacity development, and best practices on securing telecom networks against growing cyber threats and technological advancements[34]. ITU facilitates multi-stakeholder dialogues and partnerships, enabling countries to share knowledge, harmonize regulations, and build national capabilities tailored to their unique challenges and resources[37].

ITU's initiatives extend to fostering inclusive policies that consider underserved communities, women, and youth, addressing digital literacy and ensuring that cyber resilience benefits all populations equitably. Collaborative frameworks developed by ITU promote harmonized responses to cyber incidents, information sharing, and joint exercises, thereby mitigating risks at both national and international levels[38].

1.8 G8 and G20 Contributions to Cyber Terrorism Control

Terrorist groups increasingly exploit cyberspace for recruitment, propaganda, financing, and potential disruption of critical infrastructures. In response, multilateral forums such as the Group of Eight (G8) and the Group of Twenty (G20) have shaped collective approaches to counter this transnational threat of cyber terrorism. While the G8 pioneered early initiatives on high-tech crime in the late 1990s, the G20 has more recently integrated cybersecurity into its global economic governance agenda, with a particular focus on safeguarding financial systems and critical infrastructure. Together, these two forums have contributed significantly to building frameworks of cooperation, policy coordination, and capacity-building against cyber terrorism[39].

(i) G8 Initiatives:

G8 Subgroup on High-Tech Crime (1997): The G8 established the Subgroup on High-Tech Crime to address cross-border threats from computer networks. The Subgroup was tasked with promoting international cooperation in investigating and prosecuting cybercrime, developing mechanisms for the preservation of digital evidence, and encouraging harmonization of national laws.

One of the key outcomes of G8 efforts is establishment of 24/7 Network of Contact Points as an operational mechanism that enabled rapid assistance and information exchange between member states in cases involving urgent cyber threats. This network became a prototype for later global structures under the Council of Europe's Budapest Convention on Cybercrime (2001) [40].

Importantly, the Subgroup's efforts helped lay the groundwork for linking cybercrime to broader concerns about terrorism, particularly as terrorist organizations began experimenting with online propaganda and digital communication platforms in the early 2000s. The G8's early recognition of these risks positioned it as a norm-setter and paved the way for global instruments addressing the intersection of terrorism and technology[41].

The G8 also emphasized capacity-building through the sharing of best practices on digital forensics, law enforcement training, and protocols for cooperation with private technology companies.

(ii) G20 Initiatives:

The G20, comprising advanced and emerging economies, has taken up cybersecurity issues in the context of global financial stability and economic resilience. Since the mid-2010s, G20 summit communiqués have explicitly recognized the risks posed by malicious cyber activities, including their potential use by terrorist networks. The 2015 Antalya Summit committed to promoting norms of responsible state behavior in cyberspace and protecting critical infrastructure from disruption. Building on this, the 2017 Hamburg Summit underlined the importance of safeguarding the digital economy and encouraged stronger cooperation against cybercrime and cyber terrorism[42].

G20 Declarations on Cybersecurity and Critical Infrastructure Protection

The G20 has supported the UN Group of Governmental Experts (UN GGE) recommendations on norms, confidence-building measures, and capacity-building in cyberspace. The G20 Digital Economy Task Force has promoted resilience of digital infrastructure, encouraging members to adopt robust frameworks for risk assessment, incident response, and public-private collaboration. These commitments are crucial because terrorist groups have targeted critical infrastructure, such as energy grids, financial networks, and transportation systems etc. recognizing the catastrophic potential of such disruptions.

Through these declarations, the G20 has mainstreamed cybersecurity within global economic governance and signaled a collective commitment to preventing cyberspace from becoming a theater of terrorism [43].

(iii) Cooperation on Preventing Misuse of Digital Finance by Terrorist Groups

One of the most pressing intersections between cyber terrorism and global governance lies in the misuse of digital finance. Terrorist organizations have demonstrated increasing sophistication in exploiting online platforms, cryptocurrencies, and mobile payment systems to raise, transfer, and conceal funds. Recognizing these vulnerabilities, both the G8 and G20 have undertaken concerted efforts to strengthen financial oversight and mitigate risks.

The G8's early focus in the post-9/11 era centered on implementing the Financial Action Task Force (FATF) standards to combat money laundering and terrorist financing. By integrating cyber dimensions, the G8 highlighted the growing risks of anonymous digital transactions. Its recommendations encouraged member states to tighten regulatory frameworks for online financial services and enhance cooperation with the private sector to track suspicious activities[44].

The G20, given its centrality to global financial governance, has advanced this agenda further. Building on FATF guidance, the G20 has repeatedly underscored the importance of addressing vulnerabilities in the financial technology (fintech) ecosystem. The 2019 Osaka Summit reaffirmed the need for global coordination to ensure that innovations like cryptocurrencies do not provide safe havens for terrorist financing.

In addition, the G20 has supported capacity-building in developing economies, recognizing that weak financial oversight in certain jurisdictions creates systemic risks that terrorist groups can exploit. Joint training programs, technical assistance, and peer review mechanisms have sought to raise global standards of compliance and resilience. Importantly, these measures highlight the recognition that cyber terrorism is not merely a

security issue but also a financial stability concern, linking it directly to the G20's mandate[45].

(iv) Key Takeaways

The contributions of the G8 and G20 to controlling cyber terrorism reflect a complementary evolution of global governance. Both forums have also recognized the importance of public-private partnerships, legal harmonization, and capacity-building in ensuring effective responses. Although challenges remain such as uneven implementation, sovereignty concerns, and the fast-evolving nature of cyber threats the G8 and G20 together play vital roles in ensuring that the digital revolution does not become a weapon in the hands of terrorist actors[46].

Conclusion

The widespread impact of cyber-attacks on critical infrastructure has highlighted the evolving nature of cyber threats to global security, underscoring the need for a robust international legal framework to combat this growing problem. The Budapest Convention, one of the earliest instruments addressing digital offences, remains a cornerstone for global cyber law frameworks. The UN has also played a key role in shaping international legal norms, with various resolutions since 2002 addressing cyber terrorism and digital terrorism, including terrorist financing. Existing UN conventions on international security, such as the Tokyo, Hague, and Montreal Conventions, are being extended to cyber dimensions. For instance, the principles countering physical threats to aviation can be applied to cyber terrorism, where attacks on digital systems can endanger aviation safety. The ICAO's 2019 cybersecurity strategy provides a global framework for resilience, cooperation, and accountability in the digital age.

The international community has made efforts to address cyber terrorism threats, including initiatives like the G8 subgroup on High Tech Crime and G20's focus on economic stability. However, the increasing complexity of cyber threats, fueled by technological advancements, has created opportunities for malicious actors to cause significant harm with minimal consequences. To address this, legal frameworks must be continuously upgraded and effectively implemented. Harmonizing divergent national perceptions and strengthening international cooperation through a comprehensive global instrument is crucial to combating cyber terrorism.

References

Books

1. Stuart Macdonald, Thomas M. Chen, Lee Jarvis, *Cyberterrorism Understanding, Assessment, and Response*, 1st ed. (Springer, 2014).
2. Reza Montasari, *Cyberspace, Cyberterrorism and the International Security*, 1st ed. (Springer Cham, 2024).
3. Ben Brewster, Babak Akhgar, *Combatting Cybercrime and Cyberterrorism*, 1st ed. (Springer Cham, 2016).
4. The Law Library, *Protocols of 2005 to the Convention Concerning Safety of Maritime Navigation and to the Protocol Concerning Safety of Fixed Platforms on the Continental Shelf (United States Treaty)*, 19th ed. (The Law Library, 2019).
5. United Nations, *International Telecommunication Union (ITU) (UN - I-Library, 1995)*.
6. Tuba Eldem, *Global Cyberspace Security and Critical Information Infrastructure Protection*, Springer (2021).
7. A Andrianova, *Countering the Financing of Terrorism in the Conditions of Digital Economy*, Springer, Cham (2020).

Journal Articles

1. Arnaud De Borchgrave, Frank J. Cilluffo, Sharon L. Cardash, Michele M. Ledgerwood, "Cyber Threats and Information Security: Meeting the 21st Century Challenge," *NCJRS Virtual Library* 57 (2001).
2. Saman Iftikhar, "Cyberterrorism as a Global Threat: A Review on Repercussions and Countermeasures," *15 PubMed Central* 1–8 (2024).
3. Durga K., "Cyber Security Challenges to Global Peace and Justice," *3 Svadhyaya - International Journal of Transdisciplinary Research and Development (SIJTRD)* 11–9 (2024).
4. Michael L. Gross, Daphna Canetti, Dana Vashdi, "Cyber Terrorism: Its Effects on Psychological Well Being, Public Confidence and Political Attitudes," *4 ResearchGate* 1–6 (2016).
5. Jeferson Martinez Lozano, Javier M. Durán, "Software Supply Chain Attacks, a Threat to Global Cybersecurity: SolarWinds' Case Study," *11 International Journal of Safety and*
6. Hayden Coupland, "Investigating Cybercrime: The Key Jurisdictional and Technical Challenges Faced by Law Enforcement," *6* 1–27 (2022).
7. Murat Kagan Kozanhan, "Unlawful Acts Threatening Maritime Security and SUA Convention," *17 Journal of Naval Sciences and Engineering* 181–203 (2021).
8. Maryam Roshanaei, Qiang Duan, "International Telecommunication Union Standardization for Trust Provisioning in ICT Infrastructure toward Achieving UN's SDGs," *9 Journal of Computer and Communications* 44–59 (2019).

9. David Wicki-Birchler, "The Budapest Convention and the General Data Protection Regulation: Acting in Concert to Curb Cybercrime?," 1 *International Cybersecurity Law Review* 63–72 (2020).
10. Nadine Strossen, "United Nations Free Speech Standards as the Global Benchmark for Online Platforms' Hate Speech Policies," 29 *Michigan State International Law Review* 1–64 (2021).
11. Gargi Sarkar and Sandeep K. Shukla, "A framework for distinguishing cybercrime, cyberattacks, and cyberterrorism," *Journal of Economic Criminology* 4 (2024).
12. Roderic G. Broadhurst, "Developments in the global law enforcement of cyber-crime," *Policing: An International Journal* 29 (2006).
13. Hasan Cifci and Esma Ergüner Ozkoc, "Analysis of National Cybersecurity Strategies of G20," *Data & Policy* 7 (2024).
14. Sean Paul Ashley, "The Future of Terrorist Financing: Fighting Terrorist Financing in the Digital Age," *Penn State Journal of International Affairs* (2018).
15. Gaurav Dave A et al., "Cyber security challenges in aviation communication, navigation, and surveillance," *Computers & Security* 112 (2022).
16. Huidi Zhang, Jiefang Huang, "The Tokyo Convention's Journey from 1963 to the Present," *Air and Space Law* 49 (2024).
17. R. H. Mankiewicz, "The 1970 Hague Convention," *Journal of Air Law and Commerce* 37 (1971).
18. Grzegorz Zajac, "International Law Regulations Related to Combating Terrorism in Civil Aviation," *SSRN* 6 (2025).
19. Mohammad Owais Farooqui, Adnan Sarhan and Faizan Mustafa, "Aviation Cyber Security in India: Legal Gaps, International Frameworks, and Policy Reforms," *Yustisia Jurnal Hukum* 14 (2025).
20. Calvin Nobles, Darrell Burrell and Tyrone Waller, "The need for a global aviation cybersecurity defense policy," *Land Forces Academy Review* 27 (2022).

Websites / Webpages

1. United Nations Security Council, "Counter Terrorism Committee." Available at: <https://www.dagdok.org/w/dd/en/un-system/security-council/counter-terrorism-committee>
2. UN Security Council, "Security Council Resolution 1624 (2005) on Threats to International Peace and Security." Available at: <https://www.refworld.org/legal/resolution/unsc/2005/en/55500>
3. United Nations Office on Drugs and Crime, "United Nations Global Counter-Terrorism Strategy," 2018. Available at: <https://www.unodc.org/e4j/en/terrorism/module-3/key-issues/un-global-ct-strategy.html>
4. UN Security Council Counter-Terrorism Committee Executive Directorate, "Counter-Terrorism in Cyberspace," 2021. Available at: [https://www.un.org/securitycouncil/ctc/sites/www.un.org/securitycouncil.ctc/files/ctc cted factsheet ct in cyberspace oct](https://www.un.org/securitycouncil/ctc/sites/www.un.org/securitycouncil.ctc/files/ctc%20cted%20factsheet%20in%20cyberspace%20oct)
5. Alexander, "Global Cybersecurity Agenda (GCA) A Framework for International Cooperation," UNODC, 2011. Available at: [https://www.unodc.org/documents/treaties/organized crime EGM cybercrime 2011 Presentations ITU Cybercrime EGMJan2011.pdf](https://www.unodc.org/documents/treaties/organized%20crime%20EGM%20cybercrime%202011/Presentations%20ITU%20Cybercrime%20EGMJan2011.pdf)
6. Allison Pytlak, Shreya Lad, "The International Telecommunications Union (ITU) and Cyber Accountability," Stimson, 2024. Available at: <https://www.stimson.org/2024/the-international-telecommunications-union-itu-and-cyber-accountability/>
7. Council of Europe, "First Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems," 2020. Available at: <https://www.coe.int/en/web/cybercrime/first-additional-protocol>
8. Fandom, "G8 Subgroup on High-Tech Crime," 1997. Available at: https://itlaw.fandom.com/wiki/G8_Subgroup_on_High-Tech_Crime
9. John Kirton, "The G20's Growing Security Governance Success" G20 Information Centre, 2017.

Endnote

- [1] Stuart Macdonald Thomas M. Chen, Lee Jarvis, *Cyberterrorism Understanding, Assessment, and Response*, 1st ed. (Springer, 2014). [2] Ben Brewster Babak Akhgar, *Combating Cybercrime and Cyberterrorism*, 1st ed. (Springer Cham, 2016). [3] Saman Iftikhar, "Cyberterrorism as a global threat: a review on repercussions and countermeasures," 15 *pub med central* 1–8 (2024). [4] Durga.K, "CYBER SECURITY CHALLENGES TO GLOBAL PEACE AND JUSTICE," 3 *Svadhaya - International Journal of Transdisciplinary Research and Development (SIJTRD)* 11–9 (2024). [5] Michael L Gross, Daphna Canetti and Dana Vashdi, "Cyber Terrorism: Its Effects on Psychological Well Being, Public Confidence and Political Attitudes," 4 *research gate* 1–6 (2016). [6] Jefferson Martinez Lozano and Javier M. Durán, "Software Supply Chain Attacks, a Threat to Global Cybersecurity: SolarWinds' Case Study," 11 *International Journal of Safety and Security Engineering* 537–45 (2021). [7] Haekal Al Asyari, "The Evolution Of Cyberterrorism: Perspectives And Progress From The European Union And Association Of Southeast Asian Nation," 29 *Jurnal Hukum IUS QUIA IUSTUM* 1–23 (2022). [8] Hayden Coupland, "Investigating Cybercrime: The Key Jurisdictional and Technical Challenges

Faced by Law Enforcement," 6 1–27 (2022). [9] Salaheddin J. Juneidi, "Council of Europe Convention on Cyber Crime" Fifth European Intensive Programme on Information and Communication Technologies Security 1–12 (2002). [10] Jonathan Clough, "The Budapest Convention on Cybercrime and the Challenges of Harmonisation," 40 SSRN 698–736 (2015). [11] David Wicki-Birchler, "The Budapest Convention and the General Data Protection Regulation: acting in concert to curb cybercrime?," 1 International Cybersecurity Law Review 63–72 (2020). [12] Council of Europe, "First Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems," 2020.available at- <https://www.coe.int/en/web/cybercrime/first-additional-protocol> [13] Nadine Strossen, "United Nations Free Speech Standards as the Global Benchmark for Online Platforms' Hate Speech Policies," 29 Michigan State International Law Review 1–64 (2021). [14] C O'Regan, "Hate speech regulation on social media: An intractable contemporary challenge," 71 Journal of Media Law 403–29 (2018). [15] Paul Arnell & Bukola Faturoti, "The prosecution of cybercrime – why transnational and extraterritorial jurisdiction should be resisted," 37 International Review of Law, Computers & Technology 29–51 (2023). [16] Gargi Sarkar and Sandeep K. Shukla, "A framework for distinguishing cybercrime, cyberattacks, and cyberterrorism," 4 Journal of Economic Criminology 1–15 (2024). [17] United Nations Security Council., "COUNTER-TERRORISM IN CYBERSPACE."available at- https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/ctc_cted_factsheet_ct_in_cyberspace_oct_2021.pdf [18] United Nations Security Council, "Open briefing of the UN Counter-Terrorism Committee on Denying Safe Haven."available at- <https://www.un.org/securitycouncil/ctc/news/open-briefing-un-counter-terrorism-committee-denyingsafehaven-0> [19] UN Security Council, "Security Council resolution 1624 (2005) on threats to international peace and security."available at- <https://www.refworld.org/legal/resolution/unsc/2005/en/55500> [20] United Nations Office on Drugs and Crime., "United Nations Global Counter-Terrorism Strategy," 2018.available at- <https://www.unodc.org/e4j/en/terrorism/module-3/key-issues/un-global-ct-strategy.html> [21] United Nations Security Council Counter-Terrorism Committee Executive Directorate., "COUNTER-TERRORISM IN CYBERSPACE," 2021 .available at- https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/ctc_cted_factsheet_ct_in_cyberspace_oct [22] United Nation Of Council, "Maintain International Peace and Security."available at- <https://www.un.org/en/our-work/maintain-international-peace-and-security> [23] United General Assembly Nations, Resolution Adopted by the General Assembly 57/239. Creation of a Global Culture of Cybersecurity, 2003. [24] United Nations, "Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents 1973," 1035 167 (2005). [25] Reto A Dürler, "The Suppression of Unlawful Acts Against the Safety of Maritime Navigation," 3 Oxford Law Pro 428–441 (2016). [26] Murat Kagan KOZHANHAN, "UNLAWFUL ACTS THREATENING MARITIME SECURITY AND SUA CONVENTION," 17 Journal of Naval Sciences and Engineering 181–203 (2021). [27] The Law Library, Protocols of 2005 to the Convention Concerning Safety of Maritime Navigation and to the Protocol Concerning Safety of Fixed Platforms on the Continental Shelf (United States Treaty), 19th ed. (The Law Library, 2019). [28] Grzegorz Zajac, "International Law Regulations Related to Combating Terrorism in Civil Aviation," 6 SSRN 1–10 (2025). [29] Gaurav Dave A et al., "Cyber security challenges in aviation communication, navigation, and surveillance," 112 Computers & Security 1–12 (2022). [30] Georgia Lykou, George Iakovakis and Dimitris Gritzalis, "Aviation Cybersecurity and Cyber-Resilience: Assessing Risk in Air Traffic Management: Theories, Methods, Tools and Technologies," 5 research gate 245–60 (2019). [31] Pardis Moslemzadeh Tehrani, Nazura Abdul Manap and Hossein Taji, "Cyber terrorism challenges: The need for a global response to a multi-jurisdictional crime," 29 Computer Law & Security Review :207–215 (2013). [32] Mohammad Owais Farooqui, Adnan Sarhan and Faizan Mustafa, "Aviation Cyber Security in India: Legal Gaps, International Frameworks, and Policy Reforms," 14 Yustisia Jurnal Hukum 186 (2025). [33] Calvin NOBLES, Darrell BURRELL and Tyrone WALLER, "THE NEED FOR A GLOBAL AVIATION CYBERSECURITY DEFENSE POLICY," 27 Land Forces Academy Review 1–8 (2022). [34] United Nations, International Telecommunication Union (ITU) (UN - I-Library, 1995). [35] Alexander, "Global Cybersecurity Agenda (GCA) A framework for international cooperation" UNODC, 2011.available at- https://www.unodc.org/documents/treaties/organized_crime_egm_cybercrime_2011/Presentations%20ITU%20Cybercrime%20EGMJan2011.pdf [36] Maryam Roshanaei and Qiang Duan, "International Telecommunication Union Standardization for Trust Provisioning in Information, Communication and Technology Infrastructure toward Achieving United Nation's Sustainable Development Goals," 9 Journal of Computer and Communications 44–59 (2019). [37] Todor Tagarev and George Sharkov, "Multi-stakeholder Approach to Cybersecurity and Resilience," 34 Information & Security An International Journal 59–68 (2016). [38] Allison Pytlak and Shreya Lad, "The International Telecommunications Union (ITU) and Cyber Accountability" Stimson, 2024.available at-

<https://www.stimson.org/2024/the-international-telecommunications-union-itu-and-cyber-accountability/> [39] John Kirton, "The G20's Growing Security Governance Success" G20 Information Centre, 2017. [40] Fandom, "G8 Subgroup on High-Tech Crime," 1997. available at- https://itlaw.fandom.com/wiki/G8_Subgroup_on_High-Tech_Crime [41] Roderic G. Broadhurst, "Developments in the global law enforcement of cyber-crime," 29 Policing An International Journal 408–33 (2006). [42] Hasan Cifci and Esma Ergüner Ozkoc, "Analysis of National Cybersecurity Strategies of G20: objectives, latent themes, latest trends and comparisons," 7 Data & Policy 1–15 (2024). [43] Tuba Eldem, "Global Cyberspace Security and Critical Information Infrastructure Protection" Springer 1–11 (2021). [44] A Andrianova, "Countering the Financing of Terrorism in the Conditions of Digital Economy," 908 Springer, Cham 20–31 (2020). [45] Sean Paul Ashley, "The Future of Terrorist Financing: Fighting Terrorist Financing in the Digital Age" Penn State Journal of International Affairs 1–118 (2018). [46] Marina Larionova and John Kirton, "The G8–G20 relationship in global governance," 4 RESEARC GATE 1–8 (2015).