

The line between  
the digital and the  
physical world is  
being crossed with  
increasing  
frequency



750 // +1000

600 // +0

# Cyberterrorism: legal and governance challenges

by Yéelen Marie Geairon

As the digital landscape evolves at unrelenting speed and global interconnectivity deepens, terrorist groups are increasingly exploiting these dynamics with novel approaches, making cyberterrorism one of the most significant and complex threats of our time. Unlike traditional terrorist threats, bound by physical borders and material means, cyberterrorism transcends these limits, eroding security capacities, straining legal systems, and testing the resilience of international governance.

Cyberterrorism can be defined as the unlawful use of information and communication technologies (ICTs) to intimidate or coerce populations or govern-

ments for political, ideological, or religious purposes. It may take the form of cyber-attacks directly targeting computer systems, or the use of ICTs to facilitate the commission of terrorist offences, such as propaganda, financing, planning, or carrying out attacks.<sup>1</sup> Hybrid by nature, cyberterrorism often mixes traditional forms of terrorism, such as physical attacks or acts of sabotage, with digital forms of attack, such as hacking systems to gather sensitive information, executing ransomware attacks or disrupting digital or physical infrastructure. The line between the digital and the physical world is being crossed with increasing frequency, giving terrorists alternative



<sup>1</sup> United Nations Office on Drugs and Crime, "Cyberterrorism", Education for Justice (E4J) University Module Series on Cybercrime, Module 14, Key Issues. <https://www.unodc.org/e4j/zh/cybercrime/module-14/key-issues/cyberterrorism.html>

methods to execute some or all parts of their crimes, as well as disrupting investigative or preventative efforts.

In this context, tools such as generative artificial intelligence (AI) can facilitate the production of falsified content, such as *deepfakes*, to incite violence or recruit, while the *dark web* can serve as a platform for exchanging sensitive data, ranging from anonymized networking and planning of attacks, to classified information obtained through hacking and procurement of weapons (e.g., plans for 3D-printed weapons). Tools initially designed to protect privacy and the security of communications are thus being misused by terrorist groups to conceal their activities and fund their operations. AI further enables the automation of *phishing* campaigns, the tailoring of propaganda to specific target groups, and the exploitation of public information to identify technical vulnerabilities or potential targets.

In light of the rapid evolution of these criminal capabilities, recent analyses, notably by the United Nations<sup>2</sup> and the Global Centre on Cooperative Security,<sup>3</sup> have warned against terror-

ist groups using emerging technologies to target state infrastructure, particularly military, diplomatic, energy, and civil institutions. This threat has been identified by Europol in the European Union Terrorism Situation and Trend Report 2025,<sup>4</sup> in which the rise of terrorist cyber threats targeting critical infrastructure represents a growing concern.



**The fight against cyberterrorism faces a fragmented normative landscape, marked by the absence of a universal definition of terrorism and cyberterrorism**

These observations reinforce the fact that this threat cannot be measured solely in terms of its immediate impacts, but also in terms of how it challenges current legal frameworks and mechanisms governing international cooperation.

In fact, the fight against cyberterrorism faces a fragmented normative landscape, marked by the absence of a universal definition of terrorism and cyberterrorism, as well as gaps

in the rules applicable to non-state actors in cyberspace. This results in varying legal thresholds that hinder extradition, mutual legal assistance, and cross-border evidence sharing, particularly when national laws differ on the definition of offences or on double criminality requirements.

Moreover, although the Budapest Convention on Cybercrime remains a reference instrument for criminal cooperation and the preservation of electronic evidence, it is not binding on States that are not party to it, thus limiting its effectiveness on a universal scale. Similarly, United Nations Security Council Resolutions 1373 (2001) and 2462 (2019) require States to criminalize terrorist acts and disrupt their financing, including when such acts involve ICTs or virtual assets. This dimension is particularly relevant in the context of cyberterrorism, where digital platforms and cryptocurrencies can facilitate the collection and transfer of funds. Yet again, the lack of legal harmonization and the differing technical capacities of States continue to hinder the uniform application of these obligations, weakening the collective response.

2 United Nations Office of Counter-Terrorism, 2023 Counter-Terrorism Week Report, April 2023. <https://www.un.org/counterterrorism/en/2023-counter-terrorism-week>

3 Global Center on Cooperative Security, Blue Sky VI: An Independent Analysis of UN Counterterrorism Efforts, June 2023. [https://www.globalcenter.org/wp-content/uploads/Global-Center\\_Blue-Sky-VI-Report\\_June-2023.pdf](https://www.globalcenter.org/wp-content/uploads/Global-Center_Blue-Sky-VI-Report_June-2023.pdf)

4 [https://www.europol.europa.eu/cms/sites/default/files/documents/EU\\_TE-SAT\\_2025.pdf](https://www.europol.europa.eu/cms/sites/default/files/documents/EU_TE-SAT_2025.pdf)

While significant, these initiatives fail to address the persistent gaps in the legal framework applicable to non-state actors in cyberspace, particularly terrorist groups. This has fuelled the work of the Ad Hoc Intergovernmental Committee under the United Nations Office on Drugs and Crime, which led to the adoption of the [International Convention against the Criminal Use of Information Technologies by the General Assembly in 2024](#).

Pending its entry into force and in the face of the pressing threat, the response to cyberterrorism therefore still relies largely on national measures, which are often designed according to each state's own security priorities.



**The response to cyberterrorism therefore still relies largely on national measures**

While they can allow for a rapid response, these isolated approaches present two major risks. First, they undermine the international cooperation necessary for effective attribution of attacks; second, they may, in the absence of safeguards,

disproportionately restrict fundamental rights such as privacy or freedom of expression. This dual vulnerability underlines the importance of articulating operational efficiency and compliance with international standards, in particular through independent and harmonized control mechanisms.

Furthermore, ensuring that measures comply with fundamental rights is only one part of the response. Another key dimension is the effective capacity of States to investigate and prosecute the perpetrators of cyberterrorist attacks. Assigning responsibilities remains one of the major challenges, especially due to the use of relay servers, anonymization technologies and infrastructures located in third-party jurisdictions. To address this issue, national capacities must be supported by solid technical expertise, advanced tools, as well as common protocols to ensure the admissibility of evidence collected before the courts. In recognition of these challenges, Member States stressed, in Security Council resolution 2341 (2017) and in the United Nations Global Counter-Terrorism Strategy, the importance

of multi-stakeholder cooperation, involving international, regional, and subregional organizations, the private sector and civil society.<sup>5</sup>

Strengthening technical capacities and international cooperation is not only aimed at identifying and punishing perpetrators, but also at ensuring that victims receive effective protection. Indeed, the human rights dimension of the response to this threat implies considering access to justice and reparation for victims of cyberterrorist attacks, whether they are direct victims of disruptions to vital services or people affected by breaches of their personal data.

Procedures must enable them to assert their rights and obtain redress, which requires legislative and institutional frameworks adapted to the transnational and technical nature of attacks.

Hence, an effective response to cyberterrorism requires the development of integrated legal frameworks linking anti-terrorism laws and cybercrime legislation, expanded international cooperation, proactive governance of emerging technologies, and a substantial strengthening of investigative and prosecutorial capabilities.

5 During the 8th review of the Global Counter-Terrorism Strategy, the General Assembly requested “the Office of Counter-Terrorism and other relevant Global Counter-Terrorism Coordination Compact entities to jointly support innovative measures and approaches to build the capacity of Member States, upon their request, for the challenges and opportunities that new technologies provide, including the human rights aspects, in preventing and countering terrorism”.

In the face of this rapidly evolving threat in cyberspace, agility, cooperation, and the rule of law remain essential. Accordingly,

meeting the challenge of cyberterrorism requires moving beyond fragmented national approaches to build a truly

global approach that can adequately balance state sovereignty, security imperatives, and respect for fundamental rights.



## ABOUT THE AUTHOR

**Yéelen Marie Geairon** is a legal expert in counter-terrorism, defence policy, and international criminal law, with experience in governmental, parliamentary, and international organizations, including the United Nations Office of Counter-Terrorism in Rabat (Morocco), Eurojust, and the Council of Europe. Her work focuses on the intersection of security, justice, and human rights, with particular expertise in the governance of terrorism threats and associated security challenges, as well as emerging risks.

# Join

the **United Nations Interregional Crime and Justice Research Institute** and **LUMSA Human Academy** for a dynamic hybrid program to explore the ethical challenges at the intersection of AI and human rights.

Gain understanding of the impact of AI on society, public safety, personal freedom and marginalized communities.

## Info

- **Expert insights.**
- Practical **exercises** and **simulations.**
- Real-world **case studies.**
- Certificate of Participation issued by **UNICRI** and **LHA.**

This hybrid program allows for all students to have an immersive and adaptable experience, in a truly global classroom.

## SUMMER SCHOOL ON ARTIFICIAL INTELLIGENCE (AI), ETHICS AND HUMAN RIGHTS



English



Hybrid  
(Rome or Online)



Students, Post-Graduates  
and Professionals

**Foster a human-centric approach to AI,  
shape the future of technology  
and human rights!**

# Join

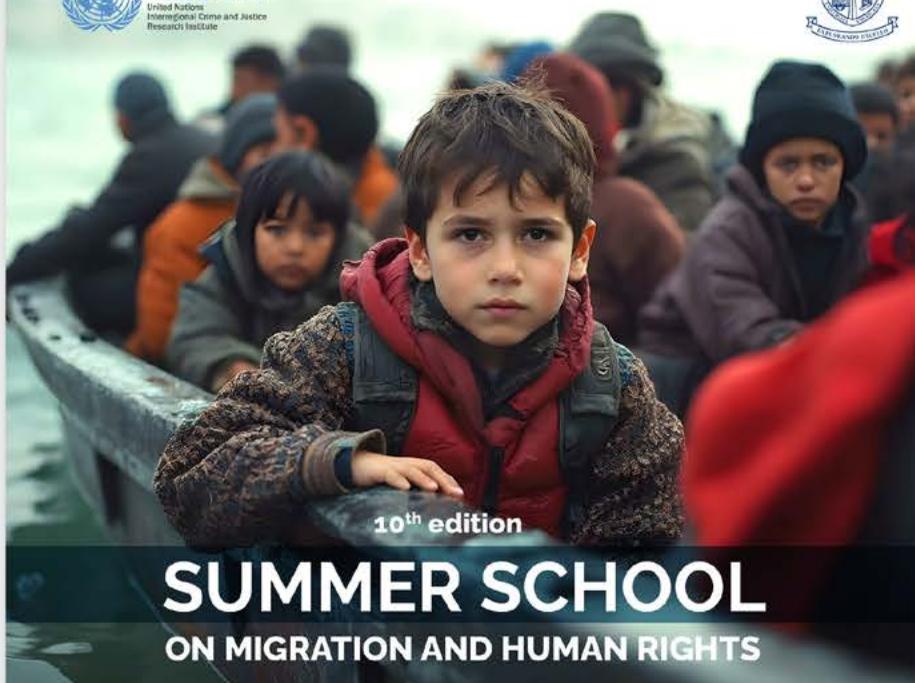
the **United Nations Interregional Crime and Justice Research Institute** and **John Cabot University** in Rome, Italy, for an immersive experience focusing on the intersection of migration, security and human rights.

Gain the legal, geopolitical and institutional tools needed to navigate one of today's most urgent global challenges.

## Info

- **Expert insights.**
- Practical **exercises** and **simulations.**
- Real-world case studies.
- Certificate of Participation issued by **UNICRI** and **JCU.**

The in-person format is ideal for those seeking to deepen their knowledge and network in the field of migration.



## SUMMER SCHOOL ON MIGRATION AND HUMAN RIGHTS



English



In-Person at JCU  
(Rome)



Students, Post-Graduates  
and Professionals

**Join the conversation.  
Shape global migration policy  
with respect for human rights!**