UNCTC - United Nations Counter Terrorism Committee

Cyberterrorism

Overview

Terrorism presents a major threat to international security and global stability. In recent years, there have been major changes to the ways in which terrorism has been conducted. While the goal of terrorism remains the same, which is “the use of violence to create a general climate of fear in a population and thereby to bring about a particular political objective." The methods in which these violent acts are conducted have changed considerably. While terrorist acts have historically been through mass-casualty events in public spaces with over 80,000 bombings and 180,000 separate terrorist acts (ex. shootings, assassinations, kidnappings) having occurred since 1970[1], technological advancements have now led to the emergence of cyberterrorism: “the politically motivated use of computers and information technology to cause severe disruption or widespread fear in society”[2]. In just the past decade, Ukraine, Estonia, and South Korea have fallen victim to major cyber-attacks targeting critical infrastructure.[3] Akin to traditional forms of terrorism, cyberterrorism strives to accomplish mass turmoil through the effective weaponization of Information and Communications Technologies (ICT), i.e. all devices that allow people and organizations to interact in the digital world.[4] These systems and devices are available to and exploited by both state and non-state actors. Exacerbated by the relative anonymity provided by the internet, cyberterrorism’s threat to international security is significant and poses a clear danger to our global stability.

---

[1] "Overview of the GTD.” Global Terrorism Database, *The University of Maryland*, www.start.umd.edu/gtd/about/

[2] “Cyberterrorism.” *Encyclopedia.com*, Encyclopedia.com, www.encyclopedia.com/humanities/dictionaries-thesauruses-pictures-and-press-releases/cyberterrorism.

[3] “Cyberterrorism .” *Wikipedia* , Wikimedia Foundation, Inc, en.wikipedia.org/wiki/Cyberterrorism.

[4] “What is Information and Communications Technology (ICT).” IGI Global, *IGI Global Inc*, www.igi-global.com/dictionary/information-and-communication-technology-ict/14316

The UN Counter-Terrorism Committee

The United Nations (UN) has worked to counter the global scourge of terrorism since the 1960s, striving to unite the international community in the fight against terrorism. The UN has focused on developing counter-terrorism legal framework to assist states in collectively working together to combat terrorism. In the aftermath of the September 2001 terrorist attacks in the United States, the United Nations Security Council unanimously adopted Resolution 1373 (2001). The resolution established a clear framework for combatting terrorism, containing multiple clauses focusing on three key areas: 1) Preventing and suppressing the financing of terrorist entities, 2) preventing states from providing any form of support to terrorist entities, including the obligation to deny safe haven and the obligation to actively work towards suppressing the recruitment of members by terrorist groups, and 3) intensifying and accelerating the sharing of operational information concerning terrorism between states.[6] The resolution further called upon states to become parties to all international counter-terrorism legal instruments.[5]

As a part of the resolution, the Counter-Terrorism Committee (CTC) was established as a subsidiary body of the United Nations Security Council (UNSC) with a global mandate to monitor, facilitate, and promote the implementation of the resolution amongst member states. The CTC works today to ensure that states implement UNSC counter-terrorism resolutions by 1) assisting states in bolstering their ability to prevent terrorism within their borders, 2) collaborating with academic, governmental, and research groups to develop a code of “good practices”, and 3) by engaging states in ongoing dialogue on counter-terrorism efforts.[6]

[5] Security Council Counter Terrorism Committee, United Nations, un.org/sc/ctc.

The Counter-Terrorism Committee and Cyberterrorism

A special focus of the CTC concerns the role of Information and Communications Technologies (ICT) in terrorism. ICT has been used by terrorist groups to commit and facilitate terrorist acts, and based on UNSC Resolutions 1373 (2001), 1624 (2005), 2129 (2013), and 2178 (2014), the mandate of the CTC includes working with states to disrupt the exploitation of ICT by terrorist groups and ensuring that states fulfill their obligation to prevent the use of ICT in enabling terrorist activities.[6]

Since 2014, the CTC has been actively working with the private sector to fulfill its mandate, and in 2016 formalized a public-private partnership called "Tech Against Terrorism." This initiative includes governments, the private sector, and academia who work together to share good practices, available tools, and through the support of larger tech platforms, assist smaller startups in taking measures that prevent its exploitation by terrorists.[6] Furthermore, the CTC continues to work with states and interested entities to preserve and enable access to digital evidence that can be used in the prosecution of foreign terrorist fighters, while continuing to monitor the developments of terrorist groups and making recommendations on strategies to combat ICT's role in terrorism.

Defining "Cyberterrorism"

There is no one concrete definition for what constitutes cyberterrorism. The concept of cyberterrorism can be divided into two distinct realms: cyber-enabled terrorism, where ICT is used to facilitate the commission of terrorist acts[7] (ex. the online recruitment of terrorists, the

[6] "Information and Communications Technologies (ICT)." *UNITED NATIONS SECURITY COUNCIL COUNTER-TERRORISM COMMITTEE EXECUTIVE DIRECTORATE (CTED)*, United Nations, www.un.org/sc/ctc/wp-content/uploads/2019/06/ctc_cted_fact_sheet_designed_ict_december_2018.pdf.
[7] "Cybercrime in Brief." *United Nations Office of Drug and Crime*, United Nations, www.unodc.org/e4j/en/cybercrime/module-1/key-issues/cybercrime-in-brief.html.

dissemination of terrorist ideologies, how-to-guides, the publishing of media that instills fear amongst citizens and/or recruits individuals to terrorist organizations, the use of deepfakes [fake images/videos that appear real]) and cyber-dependent terrorism, where ICT infrastructure is the target of the perpetrators. For example, recent history has witnessed attempts at taking over water-treatment plants, oil refineries, electrical grids, and even nuclear reactors.[8]

Attacks on ICT infrastructure that "have the capacity to cause death or bodily injury, such as explosions, disruption of hospitals, plane crashes, water contamination or that cause severe economic loss" are almost universally considered to constitute cyberterrorism.[8] However, attacks that don't have the propensity to cause physical harm, for example computer viruses and denial of service (DOS) attacks, are varyingly considered either cyberterrorism, or non-terrorist cyber-crime, by different entities.[8] The North Atlantic Treaty Organization, for example, defines cyberterrorism as "a cyberattack using or exploiting computer or communication networks to cause sufficient destruction or disruption to generate fear or to intimidate a society into an ideological goal."[8] In contrast, other organizations, such as the U.S. Federal Bureau of Investigation (FBI), define cyberterrorism as a "premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in *violence* against non-combatant targets by sub-national groups or clandestine agents."[9]

The Perpetrators of Cyberterrorism

In defining cyberterrorism, it is important to look at the various categories of perpetrators. Cyberterrorism can be carried out by:

[8] "Cyberterrorism." *Search Security*, Tech Target, searchsecurity.techtarget.com/definition/cyberterrorism.

1) Non-state actors: entities that are not carrying out an attack at the behest of, or with support from, a state. While terrorist organizations are most often associated with this category, lone wolves or any entity/individual that carries out a cyber-terrorist attack without the involvement of a state is a non-state actor.
2) Quasi-state actors: entities that carry out attacks at the behest of, or with support from, a state, but are not directly agents of the state. For example, private-citizen hackers who receive material support from states, and carry out work on their behalf, or front organizations, i.e. entities established and controlled by a state, but not publicly linked to it.
3) State actors: states who engage in cyberterrorism (attacks directly carried out by a state).

Cyber-Warfare

When state actors are involved in cyberterrorism, the question arises, when is it cyberterrorism, and when is it cyber-warfare? There exists no one clear definition of cyber-warfare nor its difference to cyberterrorism.[9] This is exacerbated by the fact that cyber-warfare and cyberterrorism do overlap.[9] One definition of cyber-warfare is a "state-on-state action equivalent to an armed attack or use of force in cyberspace that may trigger a military response with a proportional kinetic use of force."[9] Thus, state-sponsored attacks where the states <u>don't take responsibility</u> would <u>not</u> be considered "cyber-warfare," but rather cyberterrorism. The targeting of terrorist groups and related entities by states are largely considered to constitute legitimate cyber-defense.[9]

[9] Theohary, Catherine A, and John W Rollins. "Cyberwarfare and Cyberterrorism: In Brief." *Congressional Research Service*, Federation of American Scientists, 27 Mar. 2015, fas.org/sgp/crs/natsec/R43955.pdf.

Cyberterrorism: Its Past, Present, and Social Toll

Cyberterrorism is unique in its ability to easily transcend international boundaries, as attacks are carried out digitally. Thus attacks can be carried out from one corner of the world against another. Combined with the difficulties of tracing attacks back to its source, cyberterrorism poses an extreme threat. It is important to note that as of today, cyber-dependent cyberterrorism fitting the narrower definition of "causing violence" has not occurred.[10] However, there have been numerous occurrences of cyber-terrorist attacks fitting the broader NATO definition.

Cyber-terrorist attacks go back as far as 1998, when the Tamil Tigers, a Sri-Lankan terrorist group fighting for the creation of a separate state for Sri Lanka's ethnic Tamil minority, flooded Sri Lankan embassies with massive amounts of e-mails in the hopes of disrupting their communications.[11] More recently, in April 2007, Estonia was targeted in an attack that rendered the entire country offline, affecting banking, government services, health care information, and mobile networks. The attack followed a dispute between Estonia and Russia concerning the removal of a WWII-era Soviet statue from the Estonian capital. While Russia denied involvement, the evidence nonetheless suggested that they were responsible.[9] The attack illustrated the massive disruption that can occur in countries dependent on ICT (which today constitute most of the world, and disproportionally affect developing states, for example Uganda and South Africa who have strived for digitalization, but continue to lack effective cyber-defense mechanisms, given that cyber-security has been treated as an after thought compared to cyber-development) and the potentially disastrous consequences of future attacks.

---

[10] Escobar, Sophia Liemann. "What Could Cyberterrorism Look like? And Is There Such a Thing?" *Medium*, Medium , 23 Jan. 2019, medium.com/wonk-bridge/cyberterrorism-ff9285c32224.

[11] Denning, Dorothy E. "Cyberterrorism: The Logic Bomb vs the Truck Bomb." *Global Dialogue*, vol. 2, no. 4, Sept. 2000, web.archive.org/web/20130627073012/http://www.worlddialogue.org/content.php?id=111.

Cyberterrorism is also closely linked with traditional forms of terrorism. In recent years, we have seen the proliferation of the use of ICT by terrorist groups to further their causes (i.e. cyber-enabled terrorism). A notable example is the use of ICT by ISIS and affiliated organizations. Since its inception, ISIS has heavily capitalized on ICT to recruit members, spread fear, indoctrinate individuals, and disseminate its goals and values internationally, which has led to numerous ISIS-inspired terrorist attacks, for example the 2016 Berlin Truck Attack, the Charlie Hebdo Shooting, and the 2016 Nice Attack, amongst others, in the span of just a few years. In fact, it can be said that ICT was essential to ISIS' successes, thereby constituting cyber-enabled terrorism.[12] Thus, through the exploitation of ICT, ISIS was able to carry out traditional terrorist acts. While we are yet to see an act of cyber-dependent terrorism resulting in physical harm, the example of ISIS and others who currently use ICT to aid in the commission of traditional terrorist acts demonstrates the urgency of combatting cyberterrorism in all its forms.

Cyberterrorism is unique in its ability to cause widespread harm to humans, both directly and indirectly. For example, attacks on air traffic control systems and airplanes could cause accidents leading to numerous deaths. Attacks on infrastructure, such as power grids or hospitals, would also likely lead to deaths. While not an example of cyberterrorism, the Northeast Blackouts of 2003 exemplifies the effects of infrastructure damage. The blackouts, which affected much of the Eastern United States and Ontario, indirectly resulted in at least 100 deaths.[13] Were such an incident to occur as a cyber-terrorist attack, the targeting of both power grids and backup power systems would very likely lead to vast human injury and loss of life.

---

[12] Giantis, Dominika, and Dimitrios Stergious. "From Terrorism to cyberterrorism: The Case of ISIS." 7 Mar. 2018, doi:http://dx.doi.org/10.2139/ssrn.3135927.

[13] "Northeast Blackout of 2003." *Wikipedia* , Wikimedia Foundation, Inc, en.wikipedia.org/wiki/Northeast_blackout_of_2003.

Cyberterrorism also has the capacity to terrorize society through its non-loss-of-life tolls. For example, cyber-criminals have already attempted to infiltrate and compromise our financial systems, and our financial systems risk being collateral damage in cyber-terrorist attacks on national infrastructure i.e. cyberterrorism could very well cause the next financial crisis, crippling an entire nation. According to an article in the Harvard Business Review, cyberterrorism has the ability to manipulate stock exchanges, attack banks, and cause the mass-release of personal financial information; the viable targets available to cyber-terrorists are truly endless.[14] It is important to understand that almost anything involving technology is hackable. When we think of everything that involves technology, power systems, transportation, communications, military resources, and nuclear reactors, the potential impact of cyberterrorism becomes readily apparent and the consequences are disastrous.

The “Cyber" in Cyberterrorism

Cyberterrorism possesses a set of distinct features that makes its combatting more difficult than conventional forms of terrorism. First and foremost, the rapid advancements and changes in technology makes safeguarding the targets of cyberterrorism inherently more difficult. While we have established and tested guidelines on safeguarding ourselves from various forms of conventional terrorist attacks, the cyber-world is ever evolving. While new technologies come out to safeguard ICT systems, technology correspondingly comes out to circumvent those safeguards. Additionally, the remote nature of cyberterrorism makes it internationally fluid, cyber-terrorists can attack a nation without needing to ever step foot in it and both reactive and preventive responses are more complex. Cyber-attacks are often not

[14] Mee, Paul, and Til Schuermann. “How a Cyber Attack Could Cause the Next Financial Crisis.” *Harvard Business Review*, Harvard Business Publishing, 14 Sept. 2018, hbr.org/2018/09/how-a-cyber-attack-could-cause-the-next-financial-crisis.

discovered until after the attack is complete. With cyberterrorism possessing the capability to target critical global infrastructure in a single attack, the financial, social, and injury/death toll can be far higher than conventional terrorist attacks, which have been historically localized. To place the potential toll of a cyber-terrorist attack into perspective, in 2016, hackers infiltrated a US water-purification plant and altered the levels of chemicals used to treat the water. While the attack was discovered and foiled, were such an attack to successfully occur in even one plant in Montreal, for example (which has 7 plants serving 1.8 million individuals), the potential death toll would be over 250,000 [80 times that of 9/11]).[15] Furthermore, conventional counter-terrorist strategies such as preventing the flow of arms to terrorist organizations are inapplicable to cyberterrorism, and cyberterrorism is an immense threat to nations heavily reliant on ICT. As we saw with Estonia, with more essential infrastructure (think hospitals, the government, military installations etc.) connected to the digital world, a cyber-attack can be used to disrupt virtually whatever an attacker wishes to attack.[16]

The muddy waters of what constitutes cyberterrorism and what constitutes a state's legitimate, defense-oriented cyber-protection program makes the creation of a counter-cyberterrorism framework more difficult. Many nations such as the United States, Russia, China, and others have government-sponsored cyber-defense units.[17] While these units sometimes carry out attacks outside the framework of legitimate defense. For example Russia's alleged attack on Estonia, much of the work they do is legitimate, and arguably necessary to protect their states from aggression.[17] Thus, when designing framework to address cyberterrorism, consideration must be paid to states' rights to engage in cyber-related defense

[15] Leyden, J. "Water treatment plant hacked, chemical mix changed for tap supplies." The Registrar, *Situation Publishing*, 24 March 2016, https://www.theregister.co.uk/2016/03/24/water_utility_hacked/

[16] Traynor, Ian. "Russia Accused of Unleashing Cyberwar to Disable Estonia." *The Guardian*, Guardian News and Media Limited, 17 May 2007.

[17] "Cyberwarfare ." *Wikipedia* , Wikimedia Foundation, Inc, en.wikipedia.org/wiki/Cyberwarfare.

while likewise contemplating methods to prevent states from launching attacks and masking their responsibility behind a screen.

The Rise of Artificial Intelligence

The emergence of artificial intelligence (AI) has transformed the counter-terrorism landscape, as extremist organizations exploit digital platforms to spread propaganda, recruit followers, coordinate operations, and maintain virtual networks, generating vast volumes of data that challenge traditional investigative methods. Radicalization increasingly occurs through multimedia content, encrypted messaging, and algorithm-driven social media, requiring security agencies to operate in fast-moving digital environments beyond human analytical capacity. Extremist groups may also leverage AI itself, using deepfakes to inflame tensions, automated bots to amplify messaging, AI-assisted cyber-attacks, and advanced data-analysis tools for planning. This dynamic creates an evolving technological arms race between adversaries and counter-terrorism agencies.[18]

Simultaneously, AI has also therefore become a critical tool for modern counter-terrorism efforts. Machine-learning systems are capable of processing "big data" at speeds unattainable for human investigators, identifying hidden correlations, suspicious patterns, and anomalies across millions of data points. Natural-language-processing models can analyze propaganda in multiple languages, detect coded extremist terminology, and track ideological narratives across platforms. Predictive-analytics tools can assess behavioral indicators and extrapolate likely developments in a given scenario, supporting early detection and prevention efforts. These capabilities enable

[18] United Nations Office of Counter-Terrorism and United Nations Interregional Crime and Justice Research Institute. "Countering Terrorism Online with Artificial Intelligence: An Overview for Law Enforcement and Counter-Terrorism Agencies in South Asia and South-East Asia." *UNICRI*, 2021.

authorities to prioritize relevant information, significantly reduce investigative burdens, and accelerate the identification of high-risk individuals or networks.[19]

As such the future of global counter-terrorism will be defined by the ability to responsibly integrate AI into security strategies, leveraging its analytical power while ensuring safeguards against misuse, bias, or abuse.

UN Background and Issues to Consider

Numerous UN resolutions have addressed the growing threat of cyberterrorism, including Security Council resolutions 1373 (2001), 2129 (2013), and 2178 (2014) that acknowledge the threat of cyberterrorism within a larger counter-terrorism framework and recommend good-practices including urging states to combat cybercrime within their borders, enhance international information sharing, and disrupt terrorist financing.[20]

In 2025, rising geopolitical frictions in South Asia further complicated the global counter-terrorism landscape and demonstrated how traditional terrorism, cyber-enabled propaganda, and interstate rivalry can intersect to undermine international security. A series of coordinated attacks in New Delhi and Islamabad triggered severe diplomatic fallout, with India classifying the Delhi blast as a terrorist act orchestrated by "anti-national forces" operating with alleged support from Pakistan-based groups. In response, Pakistan rejected India's claims while simultaneously dealing with its own deadly attack in Islamabad, leading both nations to trade accusations across global media and diplomatic forums. [21]

---

[19] *Ibid.*
[20] "Resolutions." *United Nations Office of Counter Terrorism*, United Nations, www.un.org/counterterrorism/ctitf/en/resolutions.
[21] India Today. "Pakistan to Lead UNSC Taliban Sanctions Committee." *India Today*, 4 June 2025, https://www.indiatoday.in/world/story/pakistan-to-lead-unsc-taliban-sanctions-committee-glbs-2735342-2025-06-04
.

These tensions spilled directly into the United Nations system. India publicly questioned Pakistan's credibility as member of the CTC as well as chair of the Taliban Sanctions Committee, citing conflicts of interest and arguing that states accused of tolerating or facilitating extremist networks should not be placed in positions overseeing global sanctions regimes.[22]

We must also consider that with digitalization, especially in developing countries, cyberterrorism is no longer solely of concern to developed and technologically-connected superpowers. When cyber-security doesn't keep pace with digitalization (as is often the case), the potential list of vulnerable states grows. With digitization contributing to a more educated and financially-secure populace (both positive factors on state stability, which benefit the states themselves and the global community at large), combatting cyberterrorism is a truly global imperative, to ensure that digitalization continues to remain a goal that is admired, rather than eschewed.

Neither technology nor legal frameworks are capable of stopping cyberterrorism on their own. Legal frameworks are important for the creation of a path that will allow for the combatting of cyberterrorism, while the technology is likewise instrumental in ensuring that the tools exist to pursue the fulfillment of legal frameworks. A successful challenge to cyberterrorism necessitates the recognition of the positive aspects of technology while addressing the qualities that make it attractive to those with malicious intentions, as well as the recognition of the role of the private sector in preventing technology's exploitation. In developing frameworks to combat cyberterrorism, it is also instrumental to consider the framework's potential implication on human rights. States can potentially use laws intended to combat cyberterrorism to target

---

[22]*New Indian Express. "Pakistan at sight, India flags 'conflicts of interest' in UNSC anti-terror panels." New Indian Express, 15 Nov. 2025, ttps://www.newindianexpress.com/world/2025/Nov/15/pakistan-at-sight-india-flags-conflicts-of-interest-in-unsc-anti-terror-panels*

protestors, dissidents, and anti-government activists who use ICT to promote their ideas.[5] Thus, it is important to ensure that human rights are protected when contemplating solutions to cyberterrorism. Additionally, the largest difficulty in combatting cyberterrorism is its international nature. States cannot effectively protect themselves by focusing solely on their territory. Cyberterrorism happens across international borders, thus meaningful cooperation between the international community is a necessity to ensure the threat of cyberterrorism is successfully combatted.[23]

Delegate Questions

1. What does your country think about the issue, what unique challenges does cyberterrorism present to your country/region?
2. Is there a difference between cyberterrorism and cyber-warfare, if so, what is it? Where is the line drawn? How do we differentiate between state, quasi-state, and non-state actors? How much responsibility does/should a state possess for the actions of its citizenry?
3. How do we combat cyberterrorism while protecting digital privacy? Should certain rights be traded in the name of security? If so, to what extent, and what challenges would these pose? How do we safeguard human rights?
4. Should cyber acts that cause/have the potential to cause violence (ex cyber-warfare) be outlawed in general? How does this affect states trying to protect themselves? What implications does sovereignty have on this? What sort of regulation mechanisms should be utilized?

[23] Prasad, Krishna. "Cyberterrorism: Addressing the Challenges for Establishing an International Legal Framework." *Australian Counter Terrorism Conference*, Edith Cowan University Research Online, 5 Dec. 2012, ro.ecu.edu.au/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1016&context=act.

5. Has your country ever committed and/or been a victim to cyberterrorism? How effective are your country's cyber defenses? What are some potential solutions to this?

Suggested Links

1. www.cfr.org/expert-brief/cyberterrorism-hype-v-fact
2. www.britannica.com/topic/Cyberwarfare-The-Invisible-Threat-1729756
3. www.un.org/sc/ctc
4. https://medium.com/wonk-bridge/cyberterrorism-ff9285c32224
5. https://hbr.org/2018/09/how-a-cyber-attack-could-cause-the-next-financial-crisis
6. https://www.theguardian.com/world/2007/may/17/topstories3.russia
7. https://fas.org/sgp/crs/natsec/R43955.pdf
8. https://unicri.org/sites/default/files/2021-06/Countering%20Terrorism%20Online%20with%20AI%20-%20UNCCT-UNICRI%20Report.pdf
9. https://www.ndtv.com/world-news/india-blasts-pakistan-at-un-over-indus-waters-treaty-pahalgam-attack-20-000-indians-killed-in-terrorist-attacks-8493746