IPRI Islamabad Policy Research Institute
Research | Innovation | Dialogue | Policy

Policy Brief

Terrorism & Evolving Technologies

Khadija Almus Khanum

January 2026

Chair International Law

Executive Summary

Overview

Terrorism is being influenced continually by the rapid strides in communication, computer and military technology. While the core intent of terrorism remains unchanged, emerging tools like social media, encrypted communications, drones, Artificial Intelligence, cryptocurrencies, and additive manufacturing have changed how terrorist organisations recruit, finance, plan, and carry out attacks. By increasing reach and lowering operational barriers, these technologies function as force multipliers. Historically, terrorist groups have adapted to and exploited technological advancements. Today, these developments blur the line between physical and digital threats, leading to hybrid forms of terrorism that outpace current institutional and regulatory responses and challenge conventional counterterrorism strategies. International counterterrorism frameworks impose broad obligations on States to prevent and suppress terrorism. However, significant gaps remain. The misuse of emerging technologies by terrorists is not specifically addressed by any international instrument, and current legal frameworks mainly rely on general principles and analogy. In order to overcome these obstacles, integrated, technology-aware counterterrorism strategies must replace reactive, isolated approaches. This includes improved technical and cyber-intelligence capabilities, updated legal frameworks that make it illegal for terrorists to misuse technology, sustained capacity building across judicial and security institutions, and increased international cooperation.

Policy Recommendations

- **Strengthen Technical and Cyber-Intelligence Capabilities**: A networked cyber-intelligence system is required to link online monitoring, drone detection, and digital finance analysis. This will help spot early signs of technology-enabled terrorism. Emphasis should be placed on identifying patterns like coordinated online messages, suspicious drone activities, and digital fundraising tied to extremist groups. Monitoring extremist content in local languages across various platforms will allow for earlier disruptions and prevention.
- **Update Legal Frameworks:** Counterterrorism laws need to be updated to clearly address the misuse of new technologies by terrorist organizations. Current laws, such as Anti-Terrorism Act, do not adequately cover threats like AI-generated propaganda, autonomous or remote-controlled systems, untraceable digital weapons, or anonymous online financing. New legal provisions should target the terrorist use of these technologies rather than the technologies themselves.

- **Build Human and Institutional Capacity:** Effective counterterrorism in the digital age relies on skilled personnel in intelligence, law enforcement, prosecution, and the judiciary. Targeted training in cyber investigations, online radicalization, digital finance tracking, and evaluating digital evidence is required. Improving institutional expertise will enhance the ability to respond to changing, technology-driven terrorist threats.
- **Enhance International Cooperation and Legal Frameworks:** Technology-enabled terrorism cannot be addressed within national borders. Digital platforms, financial flows, and new technologies operate across borders. Effective response requires stronger international cooperation in sharing intelligence, exchanging digital evidence, and coordinating efforts against online terrorist networks. At the international level, Pakistan should actively push for a dedicated multilateral agreement or additional legal framework focused on the terrorist misuse of emerging technologies, building on current UN counterterrorism obligations while addressing gaps related to AI, drones, encryption, and digital finance.
- **Negotiating an International Convention on AI-Enabled Threats:** Pakistan should advocate for the negotiation of a new international convention addressing the misuse of AI for terrorist acts. The convention should establish clear definitions, attribution standards, and binding obligations for international cooperation and information-sharing. The development, facilitation, and deployment of AI-enabled tools by terrorist actors must be criminalized. The instrument should explicitly affirm meaningful human control and accountability, ensuring that human agency is not displaced in decisions affecting life, liberty, or security.

Terrorism & Evolving Technologies

Introduction

Terrorism is known to be centered on intent to cause widespread panic or harm. Despite lacking a universal legal definition, it is commonly understood as acts of violence or threats designed to instill fear, coerce governments or populations, and advance ideological or political goals.

In the context of evolving technologies, this definition expands to encompass tech-enabled methods that amplify scale, precision, or remoteness without altering the fundamental elements of criminal intent and public endangerment. Distinguishing traditional from tech-enabled threats highlights how technology shifts delivery but preserves the coercive purpose.

Understanding the nexus between terrorism and technology is crucial because terrorists increasingly exploit emerging tools like AI, drones, and encryption to enhance recruitment, planning, attacks, and financing, outpacing traditional countermeasures. This intersection also fuels the crime-terror nexus, where technologies enable hybrid threats through illicit networks and resource sharing.

Evolution of Terrorism with Technology

Throughout history, technology has proven to be a force multiplier for terrorist and insurgent groups, enabling relatively actors to exert disproportionate impact. During 19th century, anarchists, revolutionaries and nationalists quickly adapted Alfred Nobel's dynamite - originally intended for mining and construction - to carry out high-profile bombings. Similarly, mid-twentieth-century innovations such as the AK-47 rifle equipped insurgents with significantly greater firepower. The weapon was not only sold cheaply but also distributed through free production licenses to advance political objectives. Today, the seemingly indestructible AK-47 is used by around fifty standing armies around the world, is found in nearly all war zones and is readily available to insurgents and organized crime and terrorists. It is estimated to be responsible for the deaths of nearly a quarter of a million people each year.[1]

Terrorists began leveraging technology amid globalization in the late 20th century, using the internet for propaganda, recruitment, and planning by the early 2000s. Post-9/11,

[1] Susan Sim, Eric Hartunian and Paul J Milas (eds), Emerging Technologies and Terrorism: An American Perspective (US Army War College Press 2024) https://press.armywarcollege.edu/monographs/967

groups like al-Qaeda and later ISIS exploited social media and encrypted apps for global coordination and low-tech attacks, such as vehicle ramming. By the 2010s, ISIS formed drone units for surveillance and bombings, marking a shift to unmanned systems.[2]

Information and Communication Technologies ("ICTs")

In recent decades the Internet and social media have transformed terrorism. Groups such as Al-Qaeda and ISIS pioneered online propaganda and recruitment. Terrorists have used communication technologies to communicate, recruit and publicize terrorist activities. For instance, the English-language online magazine *Inspire* of Al-Qaeda provided bomb-making instructions that were used by the Boston Marathon attackers of 2013. ISIS took it a step further, creating videos of battles and executions that they released through Twitter, Facebook, and YouTube. These videos reached millions globally, through social media, spurring local and foreign fighter enlistments. Terrorists use encrypted messaging apps (for example, Telegram and WhatsApp) and even gaming or dark-web forums to coordinate in secret, illustrating how ICT lowers barriers to indoctrination and plotting.[3]

Drones/ Unmanned Aerial Vehicles ("UAVs")

The use of inexpensive commercially available drones has opened a new avenue for terrorists. Dozens of non-state actors - from ISIS and Boko Haram to Hezbollah and Houthi rebels - have deployed small quadcopters and fixed-wing drones for scouting and attacks. Once, ISIS pilots launched 70 inexpensive drones over the course of 24 hours, effectively besieging Iraqi troops and halting military movement. Drones have now become affordable weapons of terror: they are easy to pilot, carry small explosives or cameras, and can strike distant targets. UAVs have enhanced the surveillance and logistics and execution phases of attacks allowing terrorist cells to remotely hit a target with plausible deniability.[4]

[2] Seth Harrison, Evolving Tech, Evolving Terror (Center for Strategic and International Studies 2018) https://csis-website-prod.s3.amazonaws.com/s3fs-public/2022-11/180322_evolving_tech_terror_harrison.pdf?VersionId=d0YtI1fAtCt8_PtoJXLmxI.us46fCU.r ; Susan Sim, Eric Hartunian and Paul J Milas (eds), Emerging Technologies and Terrorism: An American Perspective (US Army War College Press 2024) https://press.armywarcollege.edu/monographs/967

[3] T X Hammes, 'Terror and Technology From Dynamite to Drones' War on the Rocks (4 September 2020) https://warontherocks.com/2020/09/terror-and-technology-from-dynamite-to-drones/#:~:text=conduct%20terror%20attacks%20on%20U,overall%20propaganda%20and%20recruiting%20campaign ; Antonia Ward, 'ISIS's Use of Social Media Still Poses a Threat to Stability in the Middle East and Africa' RAND (11 December 2018) https://www.rand.org/pubs/commentary/2018/12/isiss-use-of-social-media-still-poses-a-threat-to-stability.html

[4] Dr Christina Schori Liang, Terrorist Digitalis: Preventing Terrorists from Using Emerging Technologies Vision of Humanity (Global Terrorism Index 2023) https://www.visionofhumanity.org/preventing-terrorists-from-using-emerging-technologies/

Artificial Intelligence ("AI")

"Over the next decade, AI will be embraced by both terrorist organisations and counter-intelligence agencies."[5] Modern AI, especially generative models, is an emerging frontier. So far, terror groups are mostly in the exploratory stage with AI. They see potential as AI can enhance operational capabilities and propaganda efforts. Terrorist organizations are taking advantage of AI-powered technologies like generative language models, drones, autonomous vehicles, and biometric analysis to orchestrate attacks, identify high-value targets, and evade detection. AI can be used in social media outreach and persuasive messaging, as well as in the creation of deepfake videos and disinformation campaigns. These tactics help to recruit and radicalize individuals. AI assists with hacking, creating malware, and bypassing biometric security in amplifying cyber operations. Prompt engineering and open-source data allow terrorists to overcome the limitations of contemporary AI models. These trends lower technical barriers for attacks and significantly enhance precision and reach, necessitating robust counterterrorism strategies that combine technical safeguards, regulatory frameworks, and international cooperation to prevent misuse.[6]

Cryptocurrencies

Terrorist groups have turned to cryptocurrencies like Bitcoin and privacy coins such as *Monero* to finance their activities, transfer funds, and avoid traditional banking system. They have launched online donation campaigns through social media and encrypted messaging platforms. Often, they present these campaigns as humanitarian appeals for the families of fighters or detainees. They use mixers and cold wallets to hide where the money comes from.[7] Despite these tactics, blockchain analysis and law enforcement actions have allowed authorities to track and seize millions of dollars from wallets linked to terrorism.[8] This situation shows both the potential and limitations of using cryptocurrencies for financing terrorism.

[5] Institute for Economics & Peace, Global Terrorism Index 2025: Measuring the Impact of Terrorism (Sydney, March 2025) http://visionofhumanity.org/resources

[6] Clarisa Nelu, 'Exploitation of Generative AI by Terrorist Groups' International Centre for Counter-Terrorism (10 June 2024) https://icct.nl/publication/exploitation-generative-ai-terrorist-groups
; Susan Sim, Eric Hartunian and Paul J Milas (eds), Emerging Technologies and Terrorism: An American Perspective (US Army War College Press 2024) https://press.armywarcollege.edu/monographs/967

[7] TRM Team, 'Terrorist Financing: Six Crypto-Related Trends to Watch in 2023' TRM Labs Blog (15 February 2023) https://www.trmlabs.com/resources/blog/terrorist-financing-six-crypto-related-trends-to-watch-in-2023

[8] Financial Action Task Force (FATF), Crowdfunding for Terrorism Financing (Report, 31 October 2023) https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Crowdfunding-Terrorism-Financing.pdf

3D Printing

3D printing marks a significant change in technologies that aid terrorists. It represents lethal empowerment by lowering the cost, skill requirements, and detectability involved in making functional firearms and their parts. This technology increases asymmetric threats from non-state actors. Since the 2013 release of the Liberator pistol files, which were downloaded over 100,000 times within days, right-wing extremists adopted it. There have been 35 recorded incidents across 18 countries from 2017 to 2024, peaking at 11 cases in 2023. These incidents include hybrid models that compete with commercial weapons using parts from hardware stores. Motivations range from ideological defiance of gun control to supplementing arsenals, evading regulated purchases, and profit. Terrorist groups have also experimented with explosives and drone payloads, including a case linked to ISIS in the UK in 2023. By making production easier, additive manufacturing allows the creation of reliable semi-automatic weapons using transnational open-source files. This situation highlights the need for better forensics, file monitoring, and international collaboration.[9]

Emerging Terrorist Technologies and Pakistan's Security

In Pakistan, the evolving technologies have already begun to reshape the terrorism and security landscape. Militant outfits like Tehreek-e-Taliban Pakistan ("TTP"), Islamic State Khorasan Province ("ISKP") and Baloch insurgents have used drones (both for reconnaissance and limited attacks). They are getting their technical inspiration from Taliban-controlled sanctuaries in Afghanistan which are affecting border security and need new means to counter the UAVs.[10] The rise of AI generated propaganda and deepfakes has lowered the barrier for recruitment and disinformation campaigns in Urdu, Pashto and other regional languages. Online radicalization will become increasingly hard to counter without sophisticated AI-capable monitoring and rapid counter-narratives.[11] While not yet sufficiently documented

[9] Yannick Veilleux-Lepage, 'Printing Terror: An Empirical Overview of the Use of 3D-Printed Firearms by Right-Wing Extremists' Combating Terrorism Center at West Point (June 2024) https://ctc.westpoint.edu/printing-terror-an-empirical-overview-of-the-use-of-3d-printed-firearms-by-right-wing-extremists/ ; Nicolò Miotto, '3D Printing and WMD Terrorism: A Threat in the Making?' European Leadership Network (10 January 2024) https://europeanleadershipnetwork.org/commentary/3d-printing-and-wmd-terrorism-a-threat-in-the-making

[10] Rueben Dass and Abdul Basit, 'Nascent Adoption: Emerging Tech Trends by Terrorists in Afghanistan and Pakistan' (Global Network on Extremism & Technology, 18 June 2025) https://gnet-research.org/2025/06/18/nascent-adoption-emerging-tech-trends-by-terrorists-in-afghanistan-and-pakistan/

[11] Ibid.

within Pakistan, the illicit use of cryptocurrencies (especially privacy oriented coins such as *Monero*) for receiving foreign funding is becoming an emerging threat to the financial surveillance of Pakistan, prompting regulatory responses and cross-border cooperation on tracking illicit digital finance.[12] Similarly, 3D printing and other dual-use technologies, although not yet central in Pakistan's terrorism incidents, represent a plausible future threat as online weapon designs proliferate and easily accessible fabrication tools enable the production of untraceable firearm components or drone modifications.[13]

These technological trends are further enhanced by an unstable security environment including porous borders with Afghanistan that facilitate the flow of weapons, technical expertise, and fighters.[14] Tensions with India fuel narratives exploited by insurgents; and the Iran-Pakistan frontier sees cross-border militant activity often draws drone or missile response, underscoring the need for coordinated surveillance and joint counter terrorism efforts. Collectively, Pakistan has to move away from a mainly kinetic focus against terrorism to one that is multidisciplinary and tech-fluent. In particular, such a shift will entail building capabilities for cyber-intelligence, working with content moderation on online platforms to limit hate speech, and establishing anti-drone and anti-crypto capabilities. Similarly, in law, it will require updating legislation such as on digital finance and encryption regulation to counter both immediate and evolving technological threats.

International Law and the Regulation of Emerging Terrorist Technologies

Counterterrorism Obligations (UNSC Resolutions and Treaties)

Since 1963, the international community has adopted 13 conventions and 6 protocols to prevent terrorist acts. These instruments, developed under the auspices of the United Nations and the International Atomic Energy Agency ("IAEA"), are open to participation by all Member States.[15] In addition to these instruments, the UN Security Council has become

[12] Animesh Roul, 'The Rise of Monero: ISKP's Preferred Cryptocurrency for Terror Financing' (Global Network on Extremism & Technology) https://gnet-research.org/2024/10/04/the-rise-of-monero-iskps-preferred-cryptocurrency-for-terror-financing/

[13] Rajan Basra, 'The Future is Now: The Use of 3D-Printed Guns by Extremists and Terrorists' (Global Network on Extremism & Technology) https://gnet-research.org/2022/06/23/the-future-is-now-the-use-of-3d-printed-guns-by-extremists-and-terrorists/

[14] Web Desk, 'Pakistan sounds alarm on Afghan arms flow' The Express Tribune (11 November 2025) https://tribune.com.pk/story/2576919/pakistan-sounds-alarm-on-afghan-arms-flow

[15] United Nations Office of Counter-Terrorism, 'International Legal Instruments' (UN Counter-Terrorism, 2025) https://www.un.org/counterterrorism/en/international-legal-instruments

increasingly active in countering terrorism since 1999. The Council has adopted various resolutions on counter-terrorism, some of which are legally binding on UN Member States as they were adopted under Chapter VII of the UN Charter, and which form part of the core international legal framework for countering terrorism.[16]

International law, including the UN Charter, Security Council resolutions, and treaties, places significant responsibilities on States to fight terrorism. For instance, UNSC Resolution 1373 requires all States to criminalize the financing and support of terrorism and to freeze terrorist assets. These obligations include technology-driven methods of support, such as online fundraising, digital payment systems, and the misuse of communication platforms.[17] Subsequent resolutions reaffirm these duties, such as UNSCR 2178 urges States to prevent movement of foreign terrorist fighters and related support including recruitment, facilitation and coordination conducted through online platforms, encrypted communications, and other digital technologies.[18] UNSCR 2462 is another resolution which calls on States to strengthen their laws and controls to intercept the financing of terrorism, explicitly encompassing virtual assets, cryptocurrencies and other emerging financial technologies.[19] The obligations are supplemented by anti-terrorism treaties such as the Convention for the Suppression of the Financing of Terrorism, which obliges States to penalize the wilful provision or collection of funds for terrorist organizations, regardless of whether such funds are transferred through traditional banking channels or technology-driven financial mechanisms.[20]

In short, international law obligates States to "prevent and suppress" terrorism "in all its forms and manifestations". Further, States must also impose "serious criminal offences" for the punishment of support of terrorism including conduct facilitated by digital, cyber, or automated technologies. UN bodies, such as the Counter-Terrorism Committee, oversee the

[16] United Nations Office on Drugs and Crime, 'Terrorism International Framework: General UNSC Resolutions on Terrorism' (UNODC Education for Justice Law Enforcement Module, March 2019) https://www.unodc.org/cld/ru/education/tertiary/organized-crime/module-16/key-issues/terrorism-international-framework---general-unsc-resolutions-on-terrorism.html

[17] UN Security Council, 'Resolution 1373 (2001) on Threats to International Peace and Security Caused by Terrorist Acts' UN Doc S/RES/1373 (adopted 28 September 2001) https://www.unodc.org/pdf/crime/terrorism/res_1373_english.pdf

[18] UN Security Council, Resolution 2178 (2014) on threats to international peace and security caused by foreign terrorist fighters UN Doc S/RES/2178 (adopted 24 September 2014) https://docs.un.org/en/S/RES/2178%20(2014)

[19] UN Security Council, Resolution 2462 (2019) on preventing and combating the financing of terrorism UN Doc S/RES/2462 (28 March 2019) https://docs.un.org/en/S/RES/2462(2019)

[20] International Convention for the Suppression of the Financing of Terrorism (adopted 9 December 1999, opened for signature 10 January 2000, entered into force 10 April 2002) UN Doc A/RES/54/109 https://www.un.org/law/cod/finterr.htm

implementation of these norms, which are reflected in periodic resolutions calling for their full compliance.

UN Charter and Customary Law

All anti-terror measures derive authority from the UN Charter and from customary international law. For example, Article 2(4) of the Charter forbids the use of force, and Security Council action under Chapter VII makes relevant resolutions binding on States.[21] Customary principles such as non-intervention and sovereignty require States to respect the rights of other States, i.e., not allowing their territory to be used by terrorists.

State Responsibility and Due Diligence

International law holds States responsible for failing to prevent terrorist activities emanating from their territory or jurisdiction, including those enabled by emerging technologies. General principles of State responsibility impose a duty of due diligence: States must exercise "reasonable care" to prevent their territory from being used to harm other States' legal rights.

If a State knows of terrorist operations launched from within its borders, or cyber-attacks run through its networks, it must take feasible measures to terminate them. Passive support, such as permitting a group to use domestic communications or financial platforms, can breach this obligation. This principle likely extends to any harmful use of technology by terrorists (e.g., cyber-attacks, remote-controlled drones) emanating from State territory. Failing to shut down such operations, when feasible, violates the right of other States "to be free from the use of force". These duties apply in peacetime and in conflict alike. The prohibition on intervention further binds States from knowingly aiding or harboring terrorist operations.

Gaps and Emerging Issues

Despite existing international legal obligations, international law has not yet been fully adapted to some new threats. There is no dedicated treaty on AI or cyber uses by terrorists, and existing norms are applied by analogy. Furthermore, terrorists' use of emerging technologies (e.g., drones, encryption, deepfakes) may soon outpace the existing legal framework. Terrorists are increasingly using unmanned aerial systems for attacks and smuggling, but there is currently

[21] Charter of the United Nations (signed 26 June 1945, entered into force 24 October 1945) https://www.un.org/en/about-us/un-charter/full-text

no UN document that expressly prohibits the use of drones by terrorists. Similar to this, cyber tools like ransomware and online recruitment are governed by general principles, such as the prohibition the use of force, State responsibility, and evolving customary law.

The international community has recognized these challenges. The 2022 Delhi Declaration acknowledges the need "to balance fostering innovation and preventing and countering the use of new and emerging technologies … for terrorist purposes." It promotes collaborative technical solution development while upholding free information flows and human rights.[22] However, thorough and unambiguous regulations governing AI are still lacking in order to stop terrorists from abusing technology. Existing obligations under the UN Charter, international humanitarian law, human rights law, and counterterrorism law serve as the default legal guardrails, pending new international agreements and consensus.

Policy Recommendations

- **Strengthen Technical and Cyber-Intelligence Capabilities**: A networked cyber-intelligence system is required to link online monitoring, drone detection, and digital finance analysis. This will help spot early signs of technology-enabled terrorism. Emphasis should be placed on identifying patterns like coordinated online messages, suspicious drone activities, and digital fundraising tied to extremist groups. Monitoring extremist content in local languages across various platforms will allow for earlier disruptions and prevention.
- **Update Legal Frameworks:** Counterterrorism laws need to be updated to clearly address the misuse of new technologies by terrorist organizations. Current laws, such as Anti-Terrorism Act, do not adequately cover threats like AI-generated propaganda, autonomous or remote-controlled systems, untraceable digital weapons, or anonymous online financing. New legal provisions should target the terrorist use of these technologies rather than the technologies themselves.
- **Build Human and Institutional Capacity:** Effective counterterrorism in the digital age relies on skilled personnel in intelligence, law enforcement, prosecution, and the judiciary. Targeted training in cyber investigations, online radicalization, digital finance tracking, and evaluating digital evidence is required. Improving institutional expertise will enhance the ability to respond to changing, technology-driven terrorist threats.

[22] UN Security Council Counter-Terrorism Committee, Delhi Declaration on countering the use of new and emerging technologies for terrorist purposes (adopted 29 October 2022) https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2022/Dec/english_pocket_sized_delhi_declaration.final_.pdf

- **Enhance International Cooperation and Legal Frameworks:** Technology-enabled terrorism cannot be addressed within national borders. Digital platforms, financial flows, and new technologies operate across borders. Effective response requires stronger international cooperation in sharing intelligence, exchanging digital evidence, and coordinating efforts against online terrorist networks. At the international level, Pakistan should actively push for a dedicated multilateral agreement or additional legal framework focused on the terrorist misuse of emerging technologies, building on current UN counterterrorism obligations while addressing gaps related to AI, drones, encryption, and digital finance.
- **Negotiating an International Convention on AI-Enabled Threats:** Pakistan should advocate for the negotiation of a new international convention addressing the misuse of AI for terrorist acts. The convention should establish clear definitions, attribution standards, and binding obligations for international cooperation and information-sharing. The development, facilitation, and deployment of AI-enabled tools by terrorist actors must be criminalized. The instrument should explicitly affirm meaningful human control and accountability, ensuring that human agency is not displaced in decisions affecting life, liberty, or security.

Action Matrix

Options for Pakistan

Option	Pathways to Solution	Implementation of Solution	Actors Responsible	Implementation Timelines
Strengthen Technical and Cyber-Intelligence Capabilities	Integrated cyber-intelligence improves early detection of technology-enabled terrorist activity.	Establish a centralized cyber-intelligence system linking online monitoring, drone detection, and digital finance analysis; monitor extremist content in local languages.	• Intelligence Agencies • National Counter Terrorism Authority (“NACTA”) • Law Enforcement Agencies • Federal Investigation Agency (Cyber Crime Wing) • Financial Monitoring Unit (“FMU”)	6–12 months for system integration; 12–24 months for full operational use.
Update Legal Frameworks	Existing counterterrorism laws must address terrorist misuse of emerging technologies.	Amend counterterrorism legislation to cover AI-generated propaganda, autonomous systems, encrypted communications, and anonymous digital financing.	• Ministry of Law and Justice • Parliament • Judiciary • Office of the Attorney General	6–9 months for drafting; 9–18 months for enactment and enforcement.
Build Human and Institutional Capacity	Skilled personnel are essential to counter technology-driven terrorism	Provide targeted training in cyber investigations, online radicalization, drone threats, digital finance tracking, and evaluation of digital evidence.	• Law Enforcement Agencies • Judicial Academies • Intelligence Training Institutes	3–6 months to initiate training; ongoing capacity building over 12–36 months.
Enhance International Cooperation and Legal Frameworks	Cross-border terrorist use of technology requires coordinated international responses.	Strengthen intelligence-sharing and digital evidence cooperation; advocate for a multilateral framework on terrorist misuse of emerging technologies at the UN.	• Ministry of Foreign Affairs • Intelligence Agencies • NACTA • UN Counter-Terrorism Bodies	6–12 months for cooperation mechanisms; 12–36 months for multilateral legal progress.
Negotiating an International Convention on AI-Enabled Terrorist Threats	Establishing a dedicated international legal instrument to address terrorist misuse of AI technologies.	Advocate at the UN for a binding international convention criminalizing the terrorist misuse of AI, establishing clear definitions and attribution standards, mandating	• Ministry of Foreign Affairs • Permanent Mission of Pakistan to the UN	12–24 months for agenda-setting and negotiations; 3–5 years for adoption and ratification

		international cooperation, and affirming meaningful human control, accountability, and human agency in security-related decisions.	• UN General Assembly • UN Security Council Counter-Terrorism Committee (CTC) • Like-Minded States	