A double-blind, peer-reviewed, open-access, and an HEC-recognized Y-category Journal

Research Journal of Human and Social Aspects

Web link: https://rjhsa.com/index.php/rjhsa

P-ISSN: 3006-9696, **E-ISSN:** 3006-970X

Volume 4, Issue 3, 2026

Emerging Technologies and the Transformation of Terrorism: Challenges for International Security and Global Governance

Rabia Salim[1] Meena Gul[2] Fahad Khan[3]

[1] PhD Scholar, Department of Political Science, Abdul Wali Khan University, Mardan, Pakistan.

[2] PhD Scholar, Department of Pakistan Studies, Islamia College University, Peshawar, Pakistan.

[3] MPhil, Political Science, University of Peshawar, Pakistan.

Correspondence Author: salimrabia70@gmail.com

Article information

Article History:

Received: 2026-05-27

Received in revised form: 2026-06-15

Accepted: 2026-06-26

Published Online: 2026-07-22

Keywords:

Emerging Technologies; Terrorism, Artificial Intelligence; Cybersecurity; Terrorist Financing; Drones; Global Governance.

ABSTRACT

Technology, especially in its current combination of artificial intelligence and cyber tools, drones, cryptocurrencies, encrypted platforms and algorithmically-managed social media, has made repeated adaptations to terrorism, all of which have led to a terrorist practice that is vastly different in scale, speed and anonymity, disrupting traditional models of countering terrorism. This article explores the implications of technological advances for terrorist activities by examining the extent to which current governance regimes are flexible enough to address technology-enabled terrorism. A pragmatic mixed-methods design, which uses systematic document analysis, descriptive quantification of patterns of technology use, and qualitative comparative case analysis, analyses 14 documented incidents and campaigns of terror between 2016– 2025. The data sources used were United Nations documents, FATF publications, the Global Terrorism Database, Europol and INTERPOL reports, government security assessments, and peer-reviewed scholarship. While the use of AI is in its early stages, generative systems already influence how propaganda is made, how falsehoods, deceit, and translations are produced, and who the target is. Governance frameworks have been scaled up, including via the United Nations Global Counter-Terrorism Strategy, the FATF virtual-asset standards, Europol and INTERPOL collaboration and coordination, as well as the regulation of online content and by means of initiatives for the governance of AI, but implementation has been partial and non-uniform across regions, and reactive. The article adds an integrated empirical-conceptual approach to understanding the technology of terror, treating it as a collection of individual tools.

The Journal is published quarterly (March, June, September & December) by the Centre for Children Literacy and Lifelong Learning (CCLLL), Pakistan. **Web link:** https://cclll.org

Introduction

Background of the Study

Terrorism is by no means solely a technological phenomenon that remains the same as it was many years ago. Today, from nineteenth-century anarchist bombings to the transnational media campaign of the jihadist groups and the livestreamed acts of lone actors, violent non-state actors have exploited instruments that extend the reach, symbolism, and anonymity and even the lethality of their attacks (Hoffman, 2017; Nacos, 2016; Rapoport, 2004). Unlike the last 20 years, digital technologies are no longer simply enabling the glorification of violence once it has taken place; they have become even more central to the preparation and execution of violent acts, such as in structuring recruitments and financing, reconnaissance, coordination and attack execution (Conway, 2017; Cronin, 2020).

The Fourth Industrial Revolution has amplified this paradox and further exacerbated the integration of digital, cyber-physical, automated, and financial technologies into security landscapes, outpacing traditional regulation. In recent years, small business owners and individuals have seen these barriers reduced with the onset of Artificial Intelligence (AI), cyber tools, drones, blockchain transactions, cryptocurrencies, encrypted messaging, dark-web services, and algorithmic social media, as well as the increased resilience of larger organisations (Burton, 2023; INTERPOL, 2026; UNICRI & UNOCT, 2021). The importance of them is "convergence". Propaganda can be faster and more readily generated and translated, audiences can be profiled through platform 'affordances', funds can be transferred quickly via hybrid channels of cash and crypto, and coordination can move into encrypted spaces, with drugs or cyber tools extending physical reach at relatively low cost (Europol, 2025; FATF, 2023; Haugstvedt & Jacobsen, 2020).

The resulting threat is "multidirectional". AI empowers synthetic media and scalable deception, and cyber tools allow for standoffs and disruption and for extremist networks to be moved from public to semi-private and private environments; cyber tools complicate attribution and enforcement (Baele et al., 2025; Boyle), and drones provide opportunities for standoff attacks and surveillance (Baele et al., 2025).

2020; Dion-Schwarz et al., 2019; ENISA, 2024; Weimann, 2016). Such trends span the spectrum of counterterrorism, cybersecurity, financial intelligence, aviation security, border management, data protection and platform governance. Meanwhile, many of the technologies enabling and facilitating the study and commission of crimes are 'dual-use' and widely available in the global market, and are partly controlled by companies. Thus, cyber-resilience, legal regulation of financial technology and human rights protection, and co-operation with technology firms are essential for effective counterterrorism (Council of Europe, 2024; OECD, 2024; UN General Assembly, 2024). This article examines whether governance systems are adjusting rapidly enough.

Problem Statement

International anti-terrorism regimes have been primarily conceived to counter hierarchical structure, mobility of actors, "classic" methods of finance and tropical "bases. These frameworks remain relevant but have struggled to keep pace with the rapid technological progress and the decentralised nature of digital ecosystems (also known as Web 3.0) (Counter-Terrorism Committee, 2022; United Nations Security Council, 2019). Because some platforms are regulated differently, institutions are not robust, data sharing is inconsistent, and jurisdictional gaps exist between states and platforms, terrorist actors exploit these vulnerabilities. In reality, compliance is stricter in States with more sophisticated capabilities in cyber and financial intelligence, as well as in cybercrime and with intelligence agencies. Even if compliance rates are robust, the risk of threat displacement is likely to be high towards areas of poorer compliance and/or more advanced platforms (FATF, 2025; INTERPOL, 2022).

An empirical gap emanates from this governance problem. Underlying this is much previous work

that views singular technologies or singular cases of technology use in isolation, for example, online radicalisation, terrorist drone use, or cryptocurrency financing. Although important, these studies tend to downplay the extent of technological convergence across the recruitment, financing, communication, intelligence gathering, and execution of operations stages of modern terrorism (Conway, 2017; Haugstvedt & Jacobsen, 2020; Macdonald et al., 2022). There is a lack of comparative empirical studies assessing governance effectiveness across regions for multiple technologies. The current study tries to fill the gap in a mixed-methods comparative study.

Research Questions

Two research questions guide this study. RQ1 asks: How are emerging technologies transforming the operational capabilities of contemporary terrorist organisations? RQ2 asks: To what extent are existing international governance and security frameworks capable of responding effectively to technology-enabled terrorism?

Research Objectives

The first objective is to investigate how emerging technologies transform terrorist recruitment, financing, communication, operational planning, and attack execution. The second objective is to evaluate the effectiveness of international governance mechanisms in addressing technology-enabled terrorism.

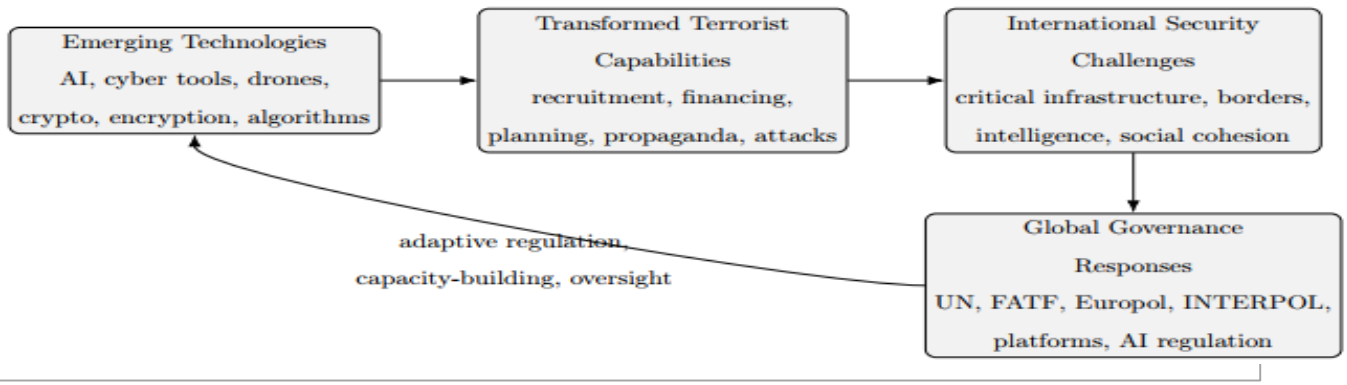
Significance of the Study

The study has both theoretical and practical implications as well as policymaking implications. Theoretically, it contributes to the study of terror in the digital age by shifting the focus of cyberterrorism out of the realm of separate discussions of Moshed idiots promoting online propaganda or a few geeks launching cyberattacks to an "integrated capability system" of technology empowering terrorism. In terms of practical application, it offers relevant information for governments, intelligence agencies, cybersecurity, financial intelligence, and tech businesses that have to respond to threats extending beyond legal and organisational limits (FATF, 2024; Europol, 2024a). The study clarifies for international organisations and policymakers the need to include both counterterrorism law and cyber norms, as well as safeguards for AI, regulation of virtual assets, and human rights measures in governance. The conceptual framework for this analysis is presented in the next subsection.

Conceptual Framework

Figure 1 captures the interplay among emerging technologies, the ability of terrorist groups to adapt to and apply them, security challenges among nations, and states' responses in global governance. The notion is that technologies and terrorism by themselves don't cause the problem. Rather, these are enabling factors that affect the cost, velocity, range, cloaking, and cooperation in terrorist acts. This means that the reconfiguration of these capacities creates framings of cross-border security issues, thereby calling for adaptive governance by the state, international bodies, tech companies, financial institutions, and civil society.

Figure 1: *Conceptual Framework Linking Emerging Technologies, Terrorism Transformation, International Security Challenges, and Global Governance Responses*



Throughout the article, the figure is followed as a guide. The literature review initially discusses the contribution of each technology to capability transformation and the response of governance systems.

Evolution of Terrorism in the Digital Age

According to the literature, there is a shift from relatively centralised organisations to networked, hybrid and decentralised mobilisations. Many network theorists expected flexible cells to utilise information flows more efficiently than hierarchical states (Arquilla & Ronfeldt, 2001). Research on jihadist social media revealed how online ecosystems afforded organisations an opportunity to convey legitimacy and for sympathy to spread, without the need for formal membership (Berger & Morgan, 2015; Klausen, 2015). However, academics warn that being radical online shouldn't be considered technologically inevitable. The interaction of these digital platforms with ideology, social networks, grievances, and offline relationships is analytically inseparable from one another; online and offline pathways are intertwined (Conway, 2017; Herath & Whittaker, 2023; Whittaker, 2022).

Artificial Intelligence and Terrorism

AI presents opportunities for terrorists and offers counterterrorism tools. AI can currently be used to facilitate the production of propaganda and translation, as well as deception, target research, and audience segmentation, all of which pose immediate risks (Europol, 2023; UNICRI & UNOCT, 2021). A large number of extremist texts and images can be generated using a generative system, and experimental results suggest that such AI-generated extremist content can be convincing to experts (Baele et al., 2025). Algorithmic recommender systems could also facilitate exposure to radicalising pathways, but this depends on the platform's design and the user's context (Burton, 2023; Ribeiro et al., 2020; Shin & Jitkajornwanich, 2024). The prevailing research view thus refutes the doom-and-gloom idea and the idea of complacency: while AI does bring benefits in terms of cost, abilities, and speed of influence, organisation, ideology and local knowledge do not go away (Department of Homeland Security, 2024). Properly written AI restrictions are crucial for AI governance, with ad hoc regulations potentially stifling acceptable research and development and addressing only lower-level, more common cases like translation, spoofing, and sea-of-knocks modifications.

Cyber Technologies and Digital Terrorism

Cyberterrorism remains contested. Whether narrow or broader, there is no single agreed-upon definition, as some definitions specify severe disruption of physical systems, while others involve coerced attacks on information systems to cause fear or pressure to secure political favours (Macdonald et al., 2022). The significance of this debate lies in two facts—first, they may present complicated problems because they can overlap with traditional cybercrime (Baker-Beall & Mott, 2022) and, second, they can seamlessly interweave components of doxing with defacement, ransomware, and propaganda (Dupont & Whelan, 2021). Empirically, it is possible to assert that the capability of terrorist groups to engage in propaganda and facilitation efforts through cyber means exceeded their destructive cyber capability and that markets such as cybercrime-as-a-service (CaaS) and ransomware reduce the barrier to entry for cyber terror (ENISA, 2024; Europol, 2024a).

Drone Technology and Autonomous Systems

The spread of UAS has made a difference in the way terrorists and insurgents can act. Commercial drones have been deployed for surveillance, propaganda imagery, and weapon delivery, particularly in conflict areas where components are readily available, and airspace is not strictly enforced (Boyle, 2020; Chavez & Swed, 2021; Rassler, 2016). The use of drones in Iraq and Syria by the Islamic State, combined

with several non-state experimentation efforts, would prove that drones could provide an air component devoid of traditional airpower (Haugstvedt & Jacobsen, 2020). But the tactically disruptive, non-state-majority drone incidents are not necessarily strategic ones, and, as such, most governance efforts should be directed toward commercial regulation, counter-drone protection, export controls, and critical-infrastructure security (Horowitz et al., 2016).

Blockchain Technology and Terrorist Financing

While traditional means of finance cash, informal value transfer, charities, front companies, and trade-based schemes continue to play a major part, blockchain-based assets provide an increased global reach, pseudonymity, and quick and easy conversion (Dion-Schwarz et al., 2019; Keatinge et al., 2018). The definitions of "virtual assets" and "virtual asset service providers" were added to the FATF standards, but there was some non-uniformity in implementation across jurisdictions (FATF, 2019, 2020, 2024). More recent estimates indicate that, while the volume of cryptocurrency exchanged by terrorists is sometimes small, it is significant in terms of its operational function (e.g., supporting propaganda infrastructure, travel, equipment, and/or logistics) (e.g., FATF, 2023, 2025; U.S. Department of the Treasury, 2024). The literature will thus align with the idea that any regulation must be based on risk, as well as with neither the perspective that cryptocurrency is high-stakes and everywhere nor the perspective that it is insignificant (Keatinge & Keen, 2020).

Encrypted Communication Technologies

One of the main factors of the resilience of terrorism is encrypted communication. Actors can sidestep takedowns and move to other platforms, such as Telegram, PM channels, dark-web forums, and smaller platforms, to regain a presence, divide their audience, coordinate supporters, and propagate within trusted networks (Bloom et al., 2019; UNODC, 2012; Weimann, 2016). The problem with encryption is that it makes it harder to conduct legitimate intelligence collection, especially in serious investigations involving terrorists. However, it simultaneously provides a defence for journalists, dissidents and others who might use it. In contrast to the early literature and media, the preference has now shifted toward targeted legal processes, platform cooperation, trust and safety measures, crisis plans, and digital forensics, rather than the weakening of encryption in general (GIFCT, 2024; Tech Against Terrorism, 2024).

Emerging Technologies and Terrorist Operational Capabilities

A large number of technologies have emerged in the literature that add value to recruitment efforts, financing, planning, propaganda, cyber operations, intelligence collection, and organisational resilience. Their primary impact is systemic–the group does not require that they be proficient with all the tools, but rather that they use some simple tools throughout the attack cycle and combine them (Cronin, 2020; Europol, 2025). This convergence explains the absence of a correlation between operational capacity and territorial disruption. It also explains how single-technology countermeasures frequently fail to target and eliminate activity, given that takedowns can lead to recruitment through the encrypted web, financial takedowns may shift fundraising to informal exchanges, and counter-drone takedowns can increase the use of cyber or propaganda functions.

International Security Challenges

Protecting against and managing terrorism – with the help of technology – burdens border and intelligence gathering, as well as the protection of critical infrastructure and the attribution of the attack's source. The proliferation of foreign terrorist fighter networks, encrypted communication, threats of drones, vulnerabilities of the cyber sphere and the online mobilisation of terrorism strain traditional security institutions (ENISA, 2024; INTERPOL, 2022; United Nations Security Council, 2017). The geopolitical and technical challenge lies in the fact that similar tools also

could be used by terrorist groups, proxies, the criminal network and state sponsors. Uncertainty of (or disputes about) the issues of attribution and the differing standards of privacy, speech and surveillance limit the ability to respond in a timely fashion, even within partners.

Global Governance Responses

Governance has been broadened, yet it is split down the middle. UN General Assembly (2023) and United Nations Security Council resolutions (2001, 2019) concerning the fight against the financing of terrorism, improved information sharing, and enhanced border security are examples of norms that guide action on these issues. Particularly in the context of terrorist use of ICT, drones and new financial technologies, the Delhi Declaration has explicitly discussed this type of misuse of technologies. Operational coordination and capacity-building efforts are in place, including by Europol and INTERPOL, which developed e-courses on AML-CFT for the virtual assets sector and crowdfunding, respectively (INTERPOL, 2024; Europol, 2025; FATF, 2025). Looking at the regional and private level, international and/or European bodies establish additional levels of governance, namely the EU terrorist-content regulation, EU AI Act, OECD AI Principles, UNESCO AI ethics recommendation, Council of Europe AI Convention, UN AI resolution, GIFCT and Tech Against Terrorism (European Parliament & Council, 2021, 2024; OECD, 2019; UNESCO, 2021; UN General Assembly, 2024; Council of Europe, 2024). They don't lack for doing anything; rather, it's the inconsistent manner in which they implement, are transparent, and are interoperable. There are several options, from sanctions to cyber forensics to platform referrals and prosecutions, which are more powerful in stronger states, but for weaker states external intelligence or ad hoc military responses may be the only option. This imbalance creates disincentives to remain in jurisdictions where enforcement is faster: terrorist actors can move their infrastructure, wallets, accounts, or facilitators to jurisdictions and platforms where enforcement is slower.

Research Gap

Previous studies have already proven that digital platforms, drones, cyber tools, virtual assets, encrypted communications and new AI are used by terrorists. However, most studies focus on technologies and/or geographic areas. But there is only a limited amount of empirical evidence that accounts for more than one technology and governance capacity across differently secure environments. This study fills this gap by coding reported incidents over the regions and analysing the issues of technology-enabled terrorism as an integrated capability system. This means that technology adoption becomes a dependent/empirical dimension of the model as it is related to governance effectiveness. This strategy is essential because technology has varying security outcomes depending on regulatory, institutional, and regional circumstances.

Research Methodology

Research Philosophy

The pragmatic research philosophy is used in this study because the research questions require answers grounded in interpretive understanding and evaluation. When a complex security issue can only be understood from a variety of epistemological stances and qualitative evidence can be translated into descriptive, quantifiable data to make policy-relevant inferences, pragmatism seems suitable. (Creswell & Plano Clark, 2018)

Research Design

The research method is a mixed-methods approach that consists of comparative qualitative case studies and a systematic analysis of documents. The qualitative part describes the use of technologies in their operational context, and the quantitative part transforms the cases' attributes into descriptive frequencies, coded in the qualitative study. This type of design cannot be said to be statistically representative; instead, it utilises structured comparison to discover emerging trends, patterns and gaps in governance that are responsive to the region.

Research Approach

Qualitative analysis techniques such as thematic analysis, comparative case analysis, and document analysis are suitable, since most incidents of the use of terrorist technology are reported in documents including policy reports, court records, intelligence summaries, sanctions notice and open-source data, and cannot be accessed directly in the field. The use of documents makes it possible to transparently triangulate official and scholarly sources, while case comparison can help pattern-match across regions and technologies (according to Bowen, 2009 and Yin, 2018). Thematic coding was conducted using standard qualitative procedural steps (Braun & Clarke, 2021), and Krippendorff (2019) determined the technology type, operational function, governance reaction, and evidentiary strength.

Case Selection

This study involved analysing 14 terrorist incidents or campaigns that featured at least one of these emerging technologies, happened between 2016 and 2025 and were already documented. The Cases span the Middle East, South Asia, Europe, and Africa to create variation in the state of technological adoption and governance capacity. Documented accounts of uses or campaigns with Islamic State drone and media activity, Houthis unmanned systems, as well as by Hamas using virtual assets to raise funds and operate drones, were included in the case pool, as were far-right livestreaming attacks, Islamic State and associated encouraged propaganda using encryption, cyber-enabled extremist activity and in Africa and South Asia more generally there were cases involving online recruitment, coordination or reconnaissance by encrypted communications. The selection criteria are summarised in Table 1.

Table 1: *Selection Criteria for Comparative Terrorism Case Studies*

Criterion	Inclusion rule	Analytical purpose
Time period	Incident or campaign documented between 2016 and 2025	Captures post-Islamic State platform migration, drone diffusion, and generative-AI emergence
Technology link	Clear evidence of AI, cyber tools, drones, virtual assets, encrypted platforms, or algorithmic social media	Ensures relevance to technology-enabled terrorism
Terrorism relevance	Actor, motive, or incident coded as terrorist or violent extremist by official, GTD, or peer-reviewed sources.	Avoids conflating ordinary cybercrime with terrorism
Regional variation	Cases drawn from the Middle East, Europe, Africa, and South Asia	Enables comparative governance analysis
Source triangulation	At least two credible source types available	Strengthens reliability and reduces single-source bias
Governance trace	Evidence of law-enforcement, regulatory, platform, financial, or international response	Allows evaluation of governance effectiveness

Data Sources

The data set was assembled using information from various sources, including United Nations reports, Financial Action Task Force (FATF) publications, Europol and INTERPOL reports, government security documents, peer-reviewed journal articles, and international security reports. In 2020, the National Consortium for the Study of Terrorism and Responses to Terrorism (START) released an upgrade to the GTD that did not include all details on the use of technology in recent attacks. An upgrade to the GTD was launched in 2020, but although the dataset is structured for event data, it does not fully capture details of technology use in recent attacks. It is therefore used only as a background tool for incident identification. Financing variables: FATF documents, European and transnational policing variables, Europol/INTERPOL documents, conceptual and tech. specific coding peer-reviewed studies.

Data Collection Procedure

For document identification, the keywords used were based on sets pertaining to technology and terrorism relief. The process of screening for relevance, date, credibility, and case specificity was applied to the sources. A matrix to code each case was used. The coding categories comprised the type of technology, the operational function of the technology, the type of actors, the region, the governance response, and the strength of evidence. When discrepancies arose, formal records were used, peer-reviewed research was preferred, and conservative coding was used for dubious statements. There was no multiplication of extreme teaching content or of extreme teaching matter.

Variables

Independent variable: emerging technologies – AI, with operationalisation of cyber capability, Virtual Assets and blockchains, encrypted communications, social media algorithms, and drones. The dependent variables include recruitment, financing, operational planning, propaganda and cyber operations. International governance capacity has been conceptualised as a moderating variable, on the basis that it influences the realisation of technological possibilities and the ongoing ability of a terrorist group to perpetrate its acts. Operationalisation is done as shown in Table 2.

Table 2: *Operationalisation of Research Variables*

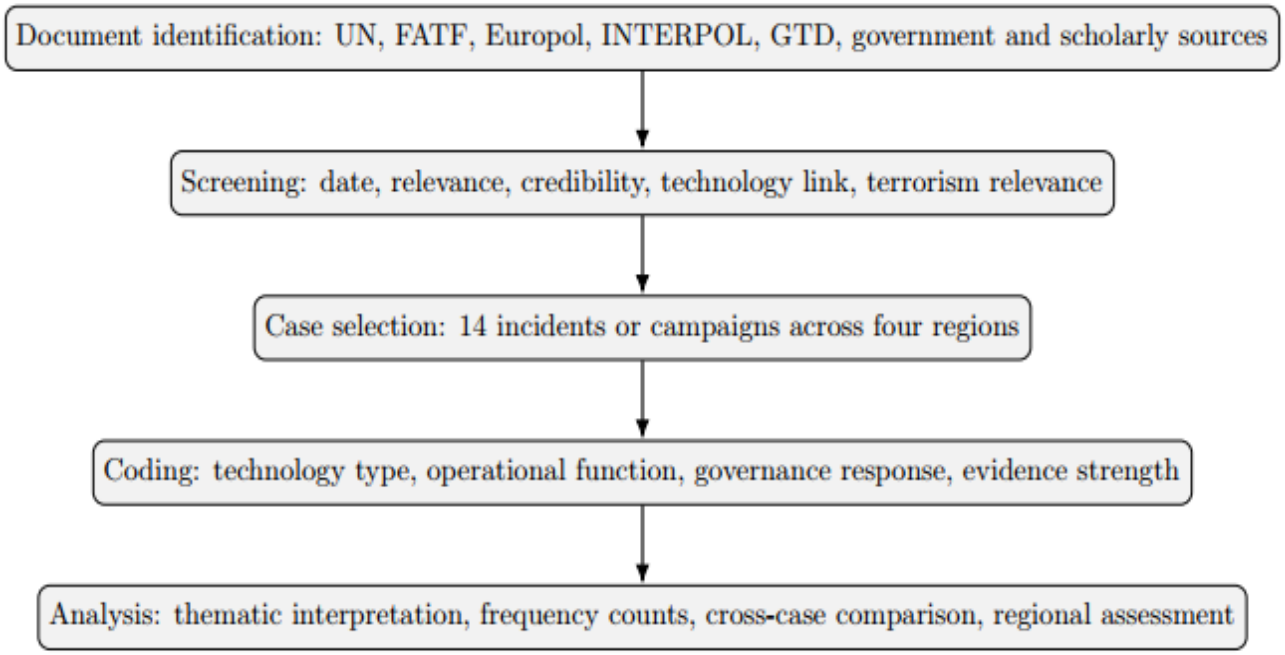
Variable type	Variable	Indicators	Coding scale
Independent	Emerging technologies	AI-generated content, cyber tools, drones, virtual assets, encrypted platforms, algorithmic amplification	Present, absent, or emerging
Dependent	Recruitment	Online radicalisation, network entry, personalised messaging, youth targeting	Low, medium, high
Dependent	Financing	Crypto solicitation, crowdfunding, informal transfers, cyber-enabled fundraising	Low, medium, high
Dependent	Operational planning	Secure coordination, reconnaissance, target research, logistics	Low, medium, high
Dependent	Propaganda	Multimedia production, livestreaming, synthetic content, cross-platform dissemination	Low, medium, high
Dependent	Cyber operations	Defacement, doxing, extortion, malware,	Low, medium,

		infrastructure targeting	high
Moderating	Governance capacity	Legal coverage, enforcement capacity, cooperation, platform engagement, financial intelligence	Weak, partial, strong

Data Analysis

These steps were followed when analysing the data. Thematic coding of documents was done as a first step. Secondly, the coded attributes were transformed into descriptive frequencies. Third, patterns were found through cross-case comparison across technology type/operational function. Fourth, a comparative regional analysis was conducted, comparing governance capacity with the level of technological adoption. The Methodological Summary is shown in Figure 2.

Figure 2: *Research Methodology Flowchart*



Reliability, Validity, and Ethical Considerations

The use of a reliable coding matrix, inclusion criteria, and the re-categorisation of cases to the source categories contributed to reliability. Triangulation was conducted using official, scholarly, and open-source materials to support validity. Examples of ethical safeguards implemented were: public availability of the secondary data, no distressing operational information that could cause harm, and no reproduction of extremist propaganda material. Thus, the methodology is balanced between transparency and sensitivity to security issues, and more harmful content is not magnified in the results section.

Results

Emerging Technologies Most Frequently Used

The following is a list of emerging technologies that are most commonly used. The cross-case analysis revealed that one tool is not predominantly used in technology-utilising crimes. Rather, cases were shown to involve multi-layered adoption, with the adoption of encrypted communication and social media ecosystems being most common. The number of cases in which coded technology was employed

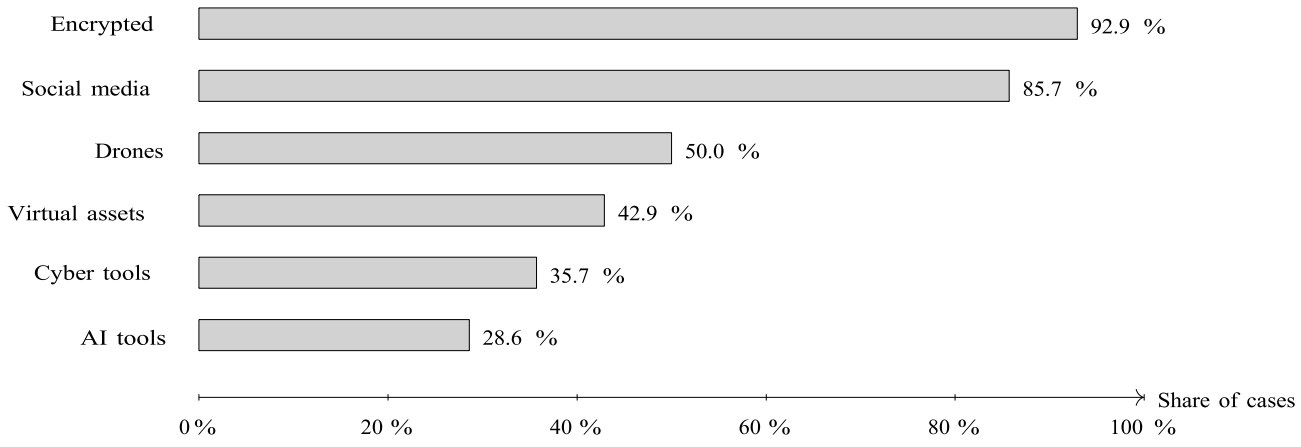
is shown in Table 3. Not only are the categories not mutually exclusive, as a single case can include many technologies, but they are also incomplete, as some technologies may not be described in the area.

Table 3: *Frequency of Emerging Technology Utilisation Across Selected Cases*

Technology category	Cases coded present	Share of cases	Dominant operational function
Encrypted communication platforms	13	92.9%	Secure coordination, propaganda continuity, audience segmentation
Social media algorithms and platform ecosystems	12	85.7%	Recruitment, amplification, identity formation, crisis exploitation
Drone or unmanned aerial systems	7	50.0%	Reconnaissance, intimidation, propaganda imagery, standoff attack capacity
Blockchain, cryptocurrency, or virtual assets	6	42.9%	Fundraising, transfer, sanctions evasion, donor outreach
Cyber tools and digital sabotage	5	35.7%	Defacement, doxing, extortion, disruption, symbolic coercion
AI or synthetic-media tools	4	28.6%	Propaganda generation, translation, deception, audience targeting

The distribution suggests that mature, accessible tech – rather than advanced AI or sophisticated cyber ops – is more widely embedded. In almost every case, encrypted platforms/social media were mentioned, as they are recognised, are cheap to access, and serve as hubs for communication. The presence of drones and virtual assets was less frequent but quite important, as it gave rise to new problems in the airspace domain related to governance, such as financial intelligence. Evidence indicated a growing reliance on AI for propaganda and deception, yet it did not suggest that there has been a systematic operation of autonomous terrorist acts by AI; the coding was still emerging. The distribution is presented as a visualisation in Figure 3.

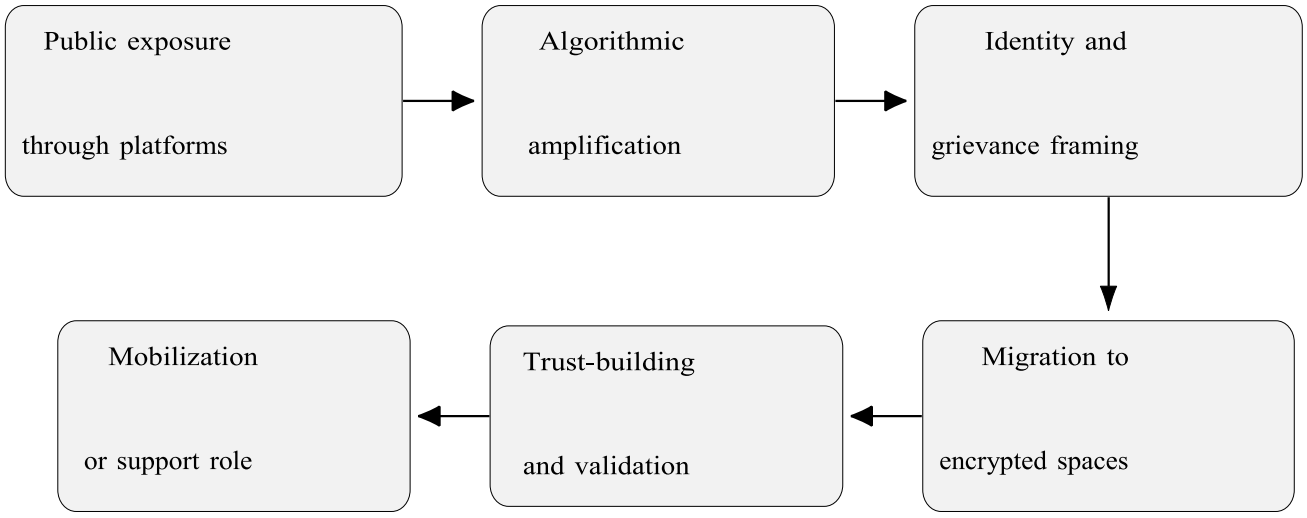
Figure 3: *Distribution of Emerging Technologies Used by Terrorist Organisations*



Impact on Terrorist Recruitment

The results indicate that recruitment is increasingly based on a more complex process of stratification and amplification, using algorithms combined with encrypted transfer and movement into closed environments. Social media platforms were the first to provide visibility, cues of identity, grievances, and emotional triggers. AI or synthetic media enabled quick adaptation of content, and encrypted channels allowed for contact after public removal of content. Essentially, this pattern falls under the umbrella of the theory that online radicalisation and offline radicalisation are not two distinct forms of radicalisation and rather than a result of either one or the other, online radicalisation or offline radicalisation must rely on the other if they wish to achieve the best possible result (Herath & Whittaker, 2023; Whittaker, 2022). The recruitment process was the same as that described in the cases and is shown in Figure 4.

Figure 4: *Technology-Enabled Terrorist Recruitment Process*



The most salient fact of copying is that it has become more modular. Not everyone who is exposed to violence becomes a victim of it – digital ecosystems are a way for supporters to step in as disseminators, donors, translators or logisticians. This is also a form of distributed participation that extends the organisation's reach even with limited physical movement.

Impact on Terrorist Financing

The type of financing via technology did not supplant traditional financing in the cases; it only added elements of speed, geographical scale, and jurisdictional complexity. When it came to crying currency and virtual assets, this combination was most relevant in online solicitation, informal exchanges, non-compliant intermediaries, or even crowdfunding. Technologies employed compared with traditional approaches are listed in Table 4.

Table 4: *Comparison of Conventional and Technology-Based Terrorist Financing Methods*

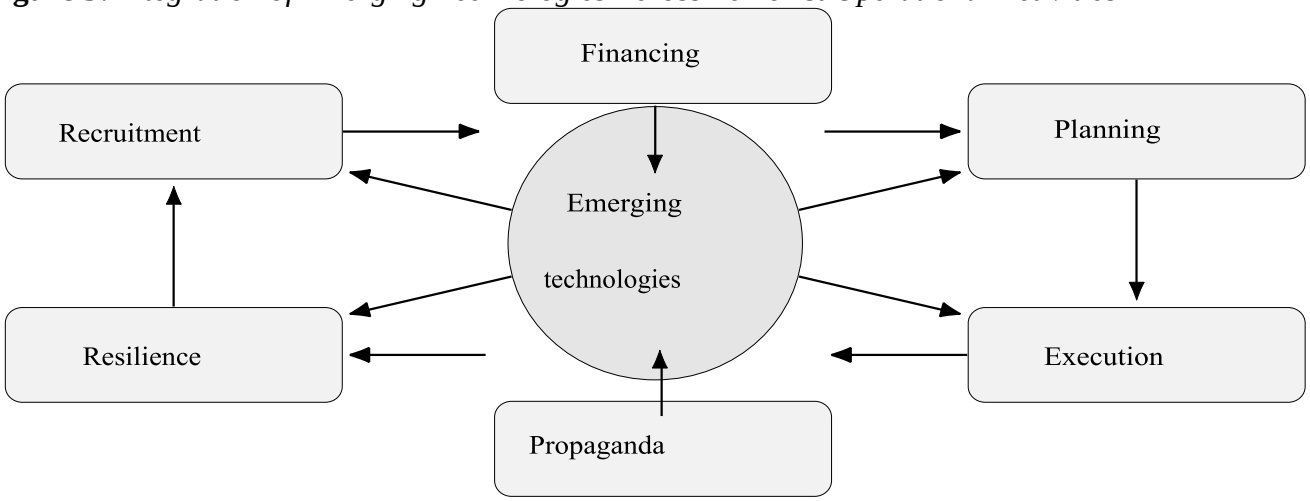
Dimension	Conventional financing	Technology-based financing
Primary channels	Cash, charities, informal value transfer, trade-based schemes, front companies	Cryptocurrency, stablecoins, crowdfunding, online payment services, social media solicitation
Visibility	Often opaque until physical transfer points are detected	Public ledger visibility may exist, but attribution is difficult without exchange and wallet intelligence
Scale	Can sustain organisations through larger diversified revenue streams	Often smaller but useful for propaganda, logistics, travel, and donor outreach
Governance tools	Sanctions, suspicious transaction reports, customs controls, financial intelligence units	VASP regulation, blockchain analytics, platform cooperation, travel-rule implementation
Key vulnerability	Human couriers, banks, charities, trade documentation	Exchange off-ramps, wallet clustering, platform records, sanctions screening

Empirically, this means that counter-financing policy shouldn't be based on the false premise that virtual assets are an exceptional field outside the framework of overall financial intelligence. The most robust responses included blockchain tracing, sanctions, exchange cooperation, crowdfunding oversight, and traditional intelligence, as highlighted by FATF in its 2023 or 2024 reports and the U.S. Department of the Treasury in its 2024 Statement.

Impact on Operational Planning and Attack Execution

While the cases illustrate the potential of emerging technologies to enhance lethality, they also show a more consistent benefit of these technologies for planning. Encrypted communications can be used to compartmentalise; compromised open-source information can support target research; the use of drones can help you get a better look at targets; cyber tools can assist with intimidation and disruption; and the use of AI can speed up the spread of disinformation. The level or relationship between technology integration and operational activities is presented in Figure 5.

Figure 5: *Integration of Emerging Technologies Across Terrorist Operational Activities*



This integration is easier to understand in terms of, say, organisations that, despite losing their territories, remain operationally resilient due to disruptions to their platforms. What's key isn't a single, impressive piece of technology; it's a distributed one in which low-cost technologies augment one another.

Comparative Regional Analysis

Regional comparison revealed that technology adoption and governance capacity vary substantially.

Table 5 summarises the regional pattern identified in the case matrix.

Table 5: *Regional Comparison of Technology Adoption and Governance Responses*

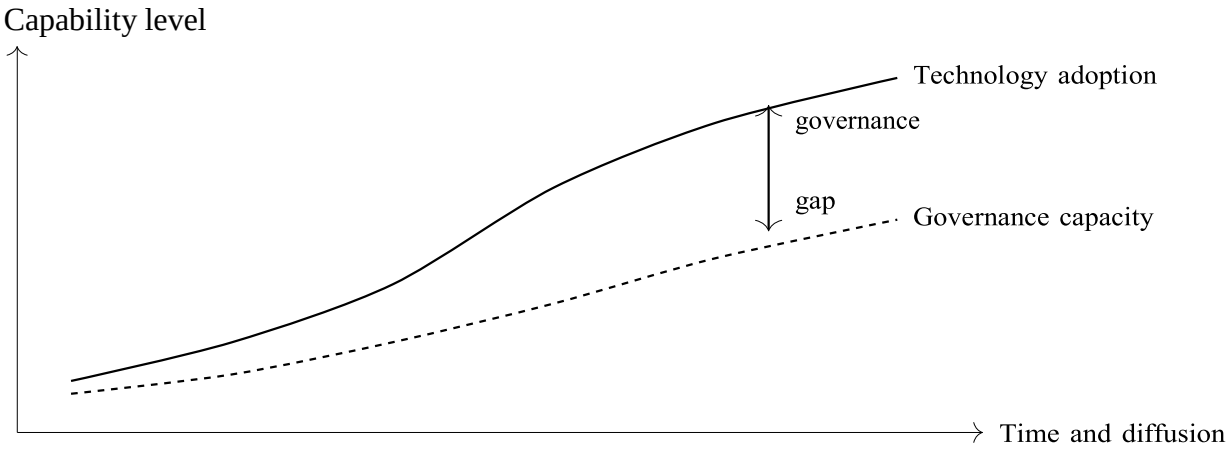
Region	Cases coded	Dominant technologies	Governance response	Main gap
Middle East	5	Drones, encrypted platforms, virtual assets, propaganda ecosystems	Military counter-drone activity, sanctions, financial intelligence, platform referrals	Proxy dynamics and conflict-zone technology diversion
Europe	4	Social media, encrypted platforms, livestreaming, AI propaganda, cyber facilitation	Europol coordination, terrorist-content regulation, prosecutions, platform cooperation	Smaller platforms, encrypted migration, youth radicalisation
Africa	3	Encrypted communication, online propaganda, drone reconnaissance, mobile money risks	INTERPOL Capacity-building, regional policing, military operations	Limited cyber forensics, weak border and financial monitoring capacity
South Asia	2	Encrypted messaging, social media recruitment, drones, digital finance channels	National counterterrorism laws, platform takedowns, border security measures	Cross-border data sharing and uneven technical capacity

Active conflict environments in the Middle East were the most diverse operational uses, as experimentation with drones and hybrid financing was possible. There was greater governance capacity in Europe, but ongoing issues with lone actors, encrypted communications, and internetwork acceleration. Limited institutional capacity can magnify the impact of relatively simple technologies in Africa and South Asia. As such, governance effectiveness will rely not solely on the law but also on implementation, digital forensics, cooperation between public and private parties, and trust in the region.

Evaluation of International Governance Responses

International governance has improved since 2019, particularly with respect to virtual-asset laws and regulations, the elimination of terrorist information, AI Ethics, and the identification of emerging technologies. However, as Figure 6 shows, this is not indicative of governance capability relative to technological development. Even if this figure is conceptual, it reflects the speed of case findings and the pace of technological accessibility relative to legislation, institutional change, budgetary considerations, training, and other forms of international cooperation, and thus the pace of change in governance capacity.

Figure 6: *Governance Capacity versus Technological Advancement Gap*



There are three implications of the governance gap. As a whole, the trend points to a reactive governance cycle with institutions' adaptation after terrorist experimentation. First, there is a growing understanding that this is an issue with international norms and inconsistent implementation. Secondly, today, private actors and financial intermediaries are key security actors, and their incentives and capacities differ. Thirdly, the developing regions are the most vulnerable to displacement as they are poorly regulated and lack scientific evidence to support their cases. These results are interwoven with the general literature.

Discussion

The results validate the core thesis of recent research on terrorism: that emerging technologies shift the opportunity structure, not so much the motivations for engaging in acts of terrorism, as the means through which motives can become terrorists' organised violence (Cronin, 2020; Hoffman, 2017). We can learn from the empirical case matrix that encrypted platforms and social media are no longer add-on services but are becoming a baseline necessity. This contributes to studies of online radicalisation, which are focused on the integrated online-offline pathway process (Herath & Whittaker, 2023; Whittaker, 2022). Meanwhile, results contradict the alarmist theories suggesting that either AI or cryptocurrency has now taken over the front line of terror. Although AI is still an emerging technology and virtual assets are still additional, both tend to pose disproportionate governance challenges – particularly regarding the scope of deception and attribution (Baele et al., 2025; FATF, 2025).

The study also shows that modularisation of terrorist organisations is taking place. Tech-

With technology, supporters can play specialised roles without having to join the organisation: propaganda dissemination, small-scale fund collection, translations, reconnaissance, or encrypted community generation and maintenance. This modularity is part of the reason explaining this phenomenon of non-organisational extinction due to the territorial defeat. The nomad's central piece becomes the networks, data and platform ecosystems (Singer & Brooking, 2018; Weimann, 2016).

Governance systems lack both the participation of all stakeholders and investment in them, and are institutionally fragmented. There are counterterrorism agencies, AML/CFT agencies, cyber agencies, aviation agencies, data protection agencies, and so on, each with its unique focus. Terrorism involving technology is transnational in nature, treating each of these aspects as aspects of a single problem. For some of this disjointment, steps have been taken by the United Nations, FATF, Europol, INTERPOL, EU regulation, the GIFCT and work in the field of AI governance, but these

organisations still have not eliminated the disjointment (Counter-Terrorism Committee, 2022; European Parliament & Council, 2021; FATF, 2024; GIFCT, 2024). Combined multi-actor structures involving legal powers, technical skills, private-sector involvement, and checks and balances against the overreach of power proved most effective in the responses identified in the case analysis.

The study's theoretical contribution is an integrated capability model of technology-enabled terrorism. The practical impact is identifying governance capacity as a moderator-technology is generative of opportunity. However, it is institutional capacity that helps or hinders the conversion of this opportunity into a sustained threat. The mixed-methods design also highlights the importance of using both methods together to interpret the cases and descriptive frequency analyses, as rare technologies (such as AI) may have low frequency yet be strategically important. In terms of international security, this translates into taking a view of CT that aligns it not just as a military and/or policing challenge but also as a cyber-financial-platform-governance challenge. Also, it must be democratic: intrusive surveillance, content moderation, and financial handling should not take place outside democratic oversight, with legal constraints, transparency, and proportionality. Governance failure in this regard can take the form of underreaction to threats and exacerbate the lack of civil liberties and accountability on platforms. Such a balance, hence, has to consider the effectiveness and the protection of rights side by side, particularly if private platforms fulfil quasi-public security functions. The discussions in the conclusion tie up these contributions and their implications.

Conclusion

In this article, the transformation in how emerging technologies enable terrorists to operate and the efficacy of existing international governance frameworks in coping with the threat were investigated. The study was a mixed-methods study, using comparative case analysis and systematic document analysis, and moving through descriptive frequencies across 14 documented incidents or campaigns ranging from 2016-2025; it found that the use of technology as a means of terrorism is best understood as a multi-technology capability system. Encrypted communications and social media ecosystems were the most prevalent technologies, while drones and virtual assets were less common but operationally relevant; cyber tools to effect hybrid disruption posed risks; and AI appeared to be a new and emerging accelerator for propaganda and deception.

The results underline the changed nature of recruitment, financing, propaganda and attack execution that has occurred with the advent of new technologies. Even as they've failed to make ideology irrelevant or replace traditional tactics of terror, they've altered the pace, impact, concealment and endurance of terrorist activities. The governance response has been scaled up with the United Nations frameworks, FATF principles and recommendations, coordination between Europol and INTERPOL, regulation of online content, and AI governance initiatives. However, the impact of such effectiveness is constrained by a lack of consistent implementation, limited regional capacity to pursue education in urban informal settlements, jurisdictional issues, reliance on the private sector, and tension within the three dimensions of security, privacy and innovation (UN General Assembly, 2023; UNESCO, 2021; United Nations Security Council, 2019).

Multiple technologies and governance mechanisms are combined in an empirical approach that both deepens understanding of terrorism and clarifies the convergence of technology and governance. Moreover, in the context of policy analysis, it reveals that governance capacity moderates the relationship between technological opportunity and terrorist effectiveness. Its basic thesis is that adaptive international governance is crucial. In today's challenging environment, threats are continually evolving due to dual-use innovation, platform migration, and transnational digital networks, and static counterterrorism tools are

insufficiently capable of meeting these threats. The governance of the future should therefore be anticipatory, evidence-based, and rights-safeguarding.

International governance should focus on adaptive security measures for AI-related extremist media, automated influence, and the misuse of AI models, without hindering legitimate research and free expression. AI providers, governments, and civil society should establish common key protocols for incident reporting, the identification of provenance, and procedures for assessment of extremist use of AI at the same time, adhering to the rights-based framework of organizations such as UNESCO, OECD, the Council of Europe and UN General Assembly (Council of Europe, 2024; OECD, 2019; UN General Assembly, 2024; UNESCO, 2021).

Real-time, cross-border sharing of information about cybersecurity incidents, joint cyber-forensic exercises, and the differentiation between cybercrime, hacktivism, and cyberterrorism should be improved. Financial intelligence units should enhance their monitoring of cryptocurrencies by strengthening supervision of VASPs in line with a risk-based approach, cooperating with exchanges, conducting blockchain analytics, and improving the implementation of the FATF standards, particularly in jurisdictions susceptible to regulatory arbitrage (FATF, 2024, 2025).

States should license and, if deemed necessary, geofence counter-drone capabilities around sensitive locations, and cooperate on export controls for all other ‘dual-use’ drone and autonomous systems, but should not restrict civilian innovation. There needs to be conditions around content-moderation standards in public–private partnerships with tech companies, that are transparent; crisis protocol, independent oversight, and assistance for platforms that don't have the resources to ensure trust and safety. Greater emphasis on providing capacity-building to developing nations needs to be included in the overall security scope of the area, instead of being a technical assistance component on the edges. Finally, counterterrorism policy should be iterative, and threat assessment, legal tools, and interinstitutional cooperation should be adjusted as technology changes. Independent review mechanisms should assess the need for such exceptional powers, including automated moderation and financial surveillance. This will help maintain and strengthen the population's confidence and lend technology-driven counterterrorism greater operational effectiveness. Recommendations should be put in place, using defined, measurable indicators, to assess the effectiveness of the cooperation and determine whether this work reduces actual risk and advances institutional mandates.

The way forward involves further research, including controlled experiments, multilingual data segmentation, and platform-specific diffusion studies of extremist propaganda generated by AI tools. Deepfake technologies must be especially highlighted in the context of credibility, incitement, identity manipulation, and misinformation in crises. It is also important to evaluate the potential for quantum computing, modern password technologies, predictive analytics, and automated systems to influence terrorist tactics over the next ten years. A comparative study of governance should be conducted to understand why some regions can take effective measures to combat terrorism using technology, while others continue to fall victim to displacement. After pressure from enforcement agencies, longitudinal studies are required to determine what changes terrorist organisations have undergone in learning to use new technologies, abandoning old ones, or adapting them. Lastly, scholars should develop legitimate methods for working with extremist material that avoid dangerous material that could be regenerated, as well as operating instructions for use in extremist operations. Future datasets must more precisely document the use of technologies than existing incident databases, ensure privacy, and rule out the swelling of extremist material. This would enable more valid causal inferences about periods of technological change and shifts in

terrorist outcomes than those currently limited to technological change.

References

Arquilla, J., & Ronfeldt, D. (Eds.). (2001). *Networks and netwars: The future of terror, crime, and militancy*. RAND Corporation.

Baele, S. J., Naserian, E., & Katz, G. (2025). Is AI-generated extremism credible? Experimental evidence from an expert survey. *Terrorism and Political Violence, 37*(8), 1060–1076. https://doi.org/10.1080/09546553.2024.2380089

Baker-Beall, C., & Mott, G. (2022). Understanding the European Union's perception of the threat of cyberterrorism: A discursive analysis. *Journal of Common Market Studies, 60*(4), 1086– 1105. https://doi.org/10.1111/jcms.13300

Berger, J. M., & Morgan, J. (2015). *The ISIS Twitter census: Defining and describing the population of ISIS supporters on Twitter*. Brookings Institution.

Bloom, M., Tiflati, H., & Horgan, J. (2019). Navigating ISIS's preferred platform: Telegram.

Terrorism and Political Violence, 31(6), 1242–1254. https://doi.org/10.1080/09546553.2017.1339695

Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal, 9*(2), 27–40.

Boyle, M. J. (2020). *The drone age: How drone technology will change war and peace*. Oxford University Press.

Braun, V., & Clarke, V. (2021). *Thematic analysis: A practical guide*. SAGE.

Burton, J. (2023). Algorithmic extremism? The securitisation of artificial intelligence and its impact on radicalism, polarisation and political violence. *Technology in Society, 75*, 102262. https://doi.org/10.1016/j.techsoc.2023.102262

Chavez, K., & Swed, O. (2021). The proliferation of drones to violent nonstate actors. *Defence Studies, 21*(1), 1–24. https://doi.org/10.1080/14702436.2020.1848426

Conway, M. (2017). Determining the role of the internet in violent extremism and terrorism: Six suggestions for progressing research. *Studies in Conflict & Terrorism, 40*(1), 77–98. https://doi.org/10.1080/1057610X.2016.1157408

Council of Europe. (2024). *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law*. Council of Europe.

Counter-Terrorism Committee. (2022). *Delhi Declaration on countering the use of new and emerging technologies for terrorist purposes*. United Nations Security Council.

Creswell, J. W., & Plano Clark, V. L. (2018). *Designing and conducting mixed methods research* (3rd ed.). SAGE.

Cronin, A. K. (2020). *Power to the people: How open technological innovation is arming tomorrow's terrorists*. Oxford University Press.

Department of Homeland Security. (2024). *Impact of artificial intelligence on criminal and illicit activities*. U.S. Department of Homeland Security.

Dion-Schwarz, C., Manheim, D., & Johnston, P. B. (2019). *Terrorist use of cryptocurrencies: Technical and organisational barriers and future threats*. RAND Corporation.

Dupont, B., & Whelan, C. (2021). Enhancing relationships between criminology and cybersecurity. *Australian & New Zealand Journal of Criminology, 54*(1), 76–92. https://doi.org/10.1177/00048658211003925

ENISA. (2024). *ENISA threat landscape 2024*. European Union Agency for Cybersecurity.

European Parliament & Council. (2021). *Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online*. Official Journal of the European Union.

European Parliament & Council. (2024). *Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence*.

Official Journal of the European Union.

Europol. (2023). *ChatGPT: The impact of large language models on law enforcement*. Europol Innovation Lab.

Europol. (2024a). *Internet Organised Crime Threat Assessment 2024*. Publications Office of the European Union.

Europol. (2024b). *Circumvention techniques employed by violent extremists to remain online*. European Counter Terrorism Centre.

Europol. (2025). *European Union Terrorism Situation and Trend Report 2025*. Publications Office of the European Union.

Fatf. (2019). *Terrorist financing risk assessment guidance*. FATF/OECD.

Fatf. (2020). *Virtual assets: Red flag indicators of money laundering and terrorist financing*. FATF/OECD.

Fatf. (2023). *Crowdfunding for terrorism financing*. FATF/OECD.

Fatf. (2024). *Targeted update on implementation of the FATF standards on virtual assets and virtual asset service providers*. FATF/OECD.

Fatf. (2025). *Comprehensive in-depth update on terrorist financing risks*. FATF/OECD.

Gifct. (2024). *Annual and transparency report 2024*. GIFCT.

Haugstvedt, H., & Jacobsen, J. O. (2020). Taking fourth-generation warfare to the skies? An empirical exploration of non-state actors' uses of weaponised unmanned aerial vehicles. *Perspectives on Terrorism, 14*(5), 26–40.

Herath, C., & Whittaker, J. (2023). Online radicalisation: Moving beyond a simple dichotomy. *Terrorism and Political Violence, 35*(5), 1027–1048. https://doi.org/10.1080/09546553.2021.1998008

Hoffman, B. (2017). *Inside terrorism* (3rd ed.). Columbia University Press.

Horowitz, M. C., Kreps, S. E., & Fuhrmann, M. (2016). Separating fact from fiction in the debate over drone proliferation. *International Security, 41*(2), 7–42.

Interpol. (2022). *Global Crime Trend Summary Report 2022*. International Criminal Police Organisation.

Interpol. (2024). *Metaverse: A law enforcement perspective*. International Criminal Police Organisation.

Interpol. (2026). *Focus: Future-facing law enforcement at the INTERPOL Innovation Centre*. International Criminal Police Organisation.

Keatinge, T., Carlisle, D., & Keen, F. (2018). *Virtual currencies and terrorist financing: Assessing the risks and evaluating responses*. European Parliament.

Keatinge, T., & Keen, F. (2020). *A sharper image: Advancing a risk-based response to terrorist financing*. Royal United Services Institute.

Klausen, J. (2015). Tweeting the jihad: Social media networks of Western foreign fighters in Syria and Iraq. *Studies in Conflict & Terrorism, 38*(1), 1–22. https://doi.org/10.1080/1057610X.2014.974948

Krippendorff, K. (2019). *Content analysis: An introduction to its methodology* (4th ed.). Sage.

Macdonald, S., Jarvis, L., & Lavis, S. M. (2022). Cyberterrorism today? Findings from a follow-on survey of researchers. *Studies in Conflict & Terrorism, 45*(8), 727–752. https://doi.org/10.1080/1057610X.2019.1696444

Nacos, B. L. (2016). *Mass-mediated terrorism: Mainstream and digital media in terrorism and counterterrorism* (3rd ed.). Rowman & Littlefield.

National Consortium for the Study of Terrorism and Responses to Terrorism. (2024). *Global Terrorism Database codebook: Inclusion criteria and variables*. University of Maryland.

OECD. (2019). *Recommendation of the Council on Artificial Intelligence*. Organisation for Economic Co-operation and Development.

OECD. (2024). *Transparency reporting on terrorist and violent extremist content online: Fourth edition*. OECD Publishing.

Rapoport, D. C. (2004). The four waves of modern terrorism. In A. K. Cronin & J. M. Ludes (Eds.),

Attacking terrorism: Elements of a grand strategy (pp. 46–73). Georgetown University Press.

Rassler, D. (2016). *Remotely piloted innovation: Terrorism, drones and supportive technology*. Combating Terrorism Centre at West Point.

Ribeiro, M. H., Ottoni, R., West, R., Almeida, V. A. F., & Meira, W. (2020). Auditing radicalisation pathways on YouTube. In *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency* (pp. 131–141). Association for Computing Machinery.

Shin, D., & Jitkajornwanich, K. (2024). How algorithms promote self-radicalisation: Audit of TikTok's algorithm using a reverse engineering method. *Social Science Computer Review, 42*(4), 1020–1040. https://doi.org/10.1177/08944393231225547

Singer, P. W., & Brooking, E. T. (2018). *LikeWar: The weaponisation of social media*. Eamon Dolan/Houghton Mifflin Harcourt.

Tech Against Terrorism. (2024). *Disrupting terrorism online in 2024*. Tech Against Terrorism.

Unesco. (2021). *Recommendation on the ethics of artificial intelligence*. United Nations Educational, Scientific and Cultural Organisation.

UN General Assembly. (2023). *The United Nations Global Counter-Terrorism Strategy: Eighth review* (A/RES/77/298). United Nations.

UN General Assembly. (2024). *Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development* (A/RES/78/265). United Nations.

Unicri & Unoct. (2021). *Algorithms and terrorism: The malicious use of artificial intelligence for terrorist purposes*. United Nations.

Unodc. (2012). *The use of the Internet for terrorist purposes*. United Nations.

United Nations Security Council. (2001). *Resolution 1373* (S/RES/1373). United Nations.

United Nations Security Council. (2017). *Resolution 2396* (S/RES/2396). United Nations.

United Nations Security Council. (2019). *Resolution 2462* (S/RES/2462). United Nations.

U.S. Department of the Treasury. (2024). *National terrorist financing risk assessment*. U.S. Department of the Treasury.

Weimann, G. (2016). *Going dark: Terrorism on the dark web*. Woodrow Wilson International Centre for Scholars.

Whittaker, J. (2022). Rethinking online radicalisation. *Perspectives on Terrorism, 16*(4), 27–40.

Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed.). SAGE.

Declaration of Conflicting Interest

The author declared no potential conflicts of interest with respect to research.

Funding Statement

No funding is received for this project.