



**How to cite this article:**

Khaleghi, A., & Khudhair Khudhair, H. A. (2025). Cyberterrorist Crimes and the Development of Counter-Terrorism Legislation: A Comparative Study of Iraqi and Iranian Law. *Journal of Historical Research, Law and Policy*, 3(4), 1-21. <https://doi.org/10.61838/jhrp.467>



Article history:  
Original Research

**Dates:**

Submission Date: 12 June 2025

Revision Date: 12 November 2025

Acceptance Date: 19 November 2025

Publication Date: 01 December 2025

# Cyberterrorist Crimes and the Development of Counter-Terrorism Legislation: A Comparative Study of Iraqi and Iranian Law

1. Abolfath. Khaleghi<sup>1</sup> : Department of Criminal Law and Criminology, Faculty of Law, University of Qom, Qom, Iran
2. Hayder Ahmed. Khudhair Khudhair<sup>2\*</sup>: Department of Criminal Law and Criminology, Faculty of Law, University of Qom, Qom, Iran

\*corresponding author's email: haider811111@gmail.com

## ABSTRACT

The rapid expansion of cyberspace has transformed the nature, methods, and scope of terrorist activity by providing terrorist actors with new tools for communication, propaganda, recruitment, financing, intelligence gathering, intimidation, espionage, and attacks against information systems and critical infrastructure. This study examines the principal types of terrorist crimes committed in cyberspace and analyzes the development of legislation designed to combat them in Iraqi and Iranian law. Using a descriptive, analytical, and comparative legal approach, the study distinguishes cyberterrorism from ordinary cybercrime by emphasizing terrorist purpose, target selection, intended consequences, and the connection between digital conduct and broader terrorist objectives. The analysis identifies major forms of cyberterrorist activity, including online dissemination of extremist content, recruitment and radicalization, terrorist communication and coordination, cyber threats, electronic espionage, terrorist financing through digital channels, unauthorized access to protected systems, data interference, and attacks against critical infrastructure. The study then evaluates the legislative frameworks of Iraq and Iran. The findings indicate that Iraq primarily relies on general anti-terrorism legislation, institutional counter-terrorism powers, and developing cybercrime rules, resulting in a relatively fragmented legal framework, particularly regarding electronic evidence, extraterritorial jurisdiction, and technologically specific offenses. Iran has developed a comparatively more established framework through computer-crime legislation, terrorist-financing regulation, and specialized cybersecurity mechanisms, although clearer integration between cybercrime provisions and terrorism-related offenses remains necessary. The comparative analysis demonstrates that both legal systems require more precise definitions of cyberterrorist conduct, stronger rules governing digital evidence, improved protection of critical infrastructure, enhanced institutional specialization, and more effective international cooperation. The study concludes that an effective legal response should be technology-neutral, proportionate, and sufficiently precise to distinguish cyberterrorism from ordinary cybercrime, hacktivism, espionage, and lawful digital expression.

**Keywords:** *Cyberterrorism; Cybercrime; Terrorist Crimes; Cyberspace; Iraqi Law; Iranian Law; Counter-Terrorism Legislation; Cybersecurity*

## Introduction

The expansion of information and communication technologies has fundamentally transformed the environments in which crime, political violence, and terrorism can be organized and carried out. Cyberspace has become an indispensable infrastructure for economic activity, public administration, communication, education, security, and



social interaction, yet the same characteristics that make digital networks valuable for legitimate purposes also make them attractive to terrorist actors. Accessibility, speed, anonymity, transnational reach, low operational cost, scalability, and the possibility of communicating without physical proximity provide terrorist organizations with capabilities that were historically unavailable through conventional forms of organization. Terrorism has therefore increasingly developed a digital dimension in which the internet is not merely an instrument for public communication but can function simultaneously as a propaganda environment, recruitment mechanism, intelligence source, organizational network, financing channel, training space, and operational platform. Research on violent extremism has consequently emphasized that the relationship between the internet and terrorism cannot be reduced to a single causal pathway, because digital platforms serve several functions at different stages of terrorist activity (1). In the Middle Eastern context, the emergence of technologically sophisticated extremist organizations has made this transformation particularly visible, and studies of ISIS have demonstrated how terrorist organizations can combine physical operations with highly developed online communication and propaganda strategies (2).

Cyberterrorism must nevertheless be distinguished from ordinary cybercrime. The technological method employed in an offense cannot by itself determine its terrorist nature. Unauthorized access to a computer, interference with digital data, theft of information, or disruption of a website may constitute ordinary cybercrime when committed for personal profit, revenge, curiosity, or other non-terrorist motives. The same conduct may acquire a terrorist character when it is carried out with the intention of intimidating a population, coercing a government, destabilizing public institutions, supporting a terrorist organization, weakening national security, or producing politically or ideologically motivated fear. The distinction is therefore based not only on the digital technique used but also on the objective, context, target, and intended consequences of the act. This hybrid structure explains why cyberterrorism presents significant conceptual and legislative difficulties. It combines the technological characteristics of cybercrime with the political and security characteristics of terrorism, thereby challenging legal systems that were originally designed to regulate these two domains separately. Regional studies have identified cyberterrorism as an increasingly serious security problem because states must simultaneously confront technically complex attacks, ideological mobilization, and the cross-border organization of violent networks (3). The broader Middle Eastern experience similarly demonstrates that cybercrime and cyberterrorism frequently overlap in their methods while remaining legally distinguishable according to purpose and impact (4).

The importance of this distinction is particularly apparent in Iraq and Iran. Both states have experienced serious security threats and have developed extensive legal and institutional responses to terrorism, while at the same time facing rapid technological change and the expansion of internet-based criminal activity. Iraq's experience has been shaped by prolonged political instability, armed conflict, the activities of terrorist organizations, the restructuring of state institutions after 2003, and significant challenges in developing effective digital governance. These conditions have placed exceptional pressure on the Iraqi legal system to respond to terrorist activity conducted through social media, digital communication systems, and other networked technologies. Cybersecurity research concerning Iraq has repeatedly emphasized structural difficulties, including deficiencies in technical capacity, institutional coordination, specialized expertise, and comprehensive legislation (5). The challenge is not merely the absence of rules. It also concerns the relationship between general anti-terrorism legislation, criminal procedure, emerging cybercrime regulation, and the technological requirements of investigation and proof. More recent analysis of Iraqi digital security has therefore highlighted the need for clearer and more coherent cybercrime legislation capable of responding to modern forms of criminal conduct (6). Capacity-building is equally important because even well-

drafted laws may remain ineffective where police, prosecutors, courts, and technical agencies lack the skills and institutional resources necessary to identify, attribute, preserve, and analyze digital evidence (7).

Iran presents a different but related legal experience. The Iranian legal system has developed specific legislation governing computer crimes and has created institutional mechanisms for cybersecurity and digital surveillance, while terrorism has traditionally been addressed through broader criminal, national-security, and religiously derived categories. Iran's experience demonstrates that the existence of cybercrime legislation does not automatically create a comprehensive legal framework for cyberterrorism. The relationship between computer offenses, terrorism, national-security crimes, terrorist financing, and attacks against strategically important infrastructure must still be defined with sufficient precision. Analysis of Iran's cybersecurity framework has identified both the development of specialized legal rules and continuing concerns regarding the adaptation of those rules to contemporary cyber threats (8). Iran's wider counter-terrorism position has also evolved under the influence of domestic security concerns and the international legal environment, creating a complex interaction between national criminal policy and broader global counter-terrorism expectations (9). These circumstances make Iran a particularly useful comparator for Iraq because the two legal systems face similar regional threats but have developed different degrees of institutionalization and legislative specialization.

The contemporary threat environment further confirms that cyberterrorism cannot be analyzed exclusively through traditional concepts of malicious software or website attacks. The digital dimension of political and military conflict has expanded to include hacktivism, disinformation, artificial intelligence-assisted operations, cyber-enabled intelligence collection, and attacks that blur the boundaries among terrorism, cyber warfare, espionage, sabotage, and politically motivated cybercrime. Recent analysis has described a new phase of hacktivism in which loosely coordinated digital actors can become involved in geopolitical conflicts and conduct operations capable of producing significant political and psychological effects (10). Developments in artificial intelligence also create the possibility of accelerating cyber operations, enhancing automated targeting, generating persuasive propaganda, supporting social engineering, and increasing the scale of malicious digital activity (11). These developments are especially important for legal systems because conventional statutory definitions may focus on particular technologies or specific forms of interference and may therefore become obsolete when new methods emerge. Recent scholarship examining low-level cyberattacks in armed and political conflicts has also demonstrated that numerous cyber operations may produce limited direct physical damage while still contributing to intimidation, disruption, propaganda, and strategic pressure (12). The legal problem is therefore not simply how to criminalize the most destructive attack but how to identify the threshold at which digitally enabled conduct becomes part of terrorist activity.

Another important characteristic of cyberterrorist offenses is their transnational nature. A perpetrator may operate in one country, use infrastructure located in several other jurisdictions, target systems in a different state, communicate through multinational digital platforms, and conceal identity through technical mechanisms that complicate attribution. This structure weakens the effectiveness of purely territorial approaches to criminal law. Investigation may require rapid preservation of data held abroad, cooperation among law-enforcement authorities, extradition arrangements, shared technical standards, and recognition of electronic evidence generated in foreign jurisdictions. Cybersecurity has therefore raised important questions under international law regarding sovereignty, jurisdiction, state responsibility, cross-border investigation, and international cooperation (13). The role of international treaties and cooperative legal frameworks is particularly important in cyberterrorism because no state

can effectively investigate or prosecute all dimensions of a transnational digital offense without external assistance (14). For Iraq and Iran, this problem is intensified by political conditions, regional rivalries, sanctions, differences in legal systems, and varying levels of cooperation with international institutions.

The protection of critical infrastructure represents another central concern. Cyberterrorism becomes especially serious when terrorist actors target electricity networks, water systems, transportation infrastructure, banking services, telecommunications, military systems, government databases, or other facilities whose disruption can affect large populations. In such cases, the harm may extend beyond loss of data and include economic instability, interruption of essential services, public panic, damage to national defense capabilities, or physical consequences. Studies of cybersecurity in the Middle East have long emphasized the gap between increasing levels of technological dependence and the capacity of states to protect vulnerable infrastructure (15). The evolution of regional cyber threats similarly demonstrates that attacks may be directed at a wide variety of governmental, commercial, and strategic systems (16). The legal response must therefore address not only completed destructive attacks but also preparatory activity, attempted interference, unlawful acquisition of protected information, support for terrorist cyber operations, and coordination among participants.

The digital transformation of terrorism also requires attention to propaganda, recruitment, and ideological mobilization. Terrorist organizations may use online platforms to disseminate narratives, glorify violence, communicate ideological justifications, identify potential recruits, establish virtual communities, and maintain contact with supporters who never physically enter a terrorist-controlled territory. The concept of “cyber jihad” illustrates how terrorist actors can exploit the internet as part of a broader political and ideological strategy rather than merely as a technical instrument (17). Online propaganda may also serve as a bridge between ideological radicalization and practical terrorist support by directing users toward encrypted communication channels, training materials, financial mechanisms, or operational networks. Yet criminalizing such activity raises difficult questions concerning the boundary between punishable terrorist incitement or support and protected expression. Overly broad provisions may undermine freedom of expression, while excessively narrow rules may allow deliberate terrorist facilitation to escape criminal responsibility. Effective legislation must therefore establish sufficiently precise criteria for terrorist intent, prohibited conduct, and the required connection between online activity and terrorist objectives.

Technological capacity also affects the effectiveness of legislation. Developing states may adopt formal cybercrime laws without possessing adequate forensic laboratories, trained investigators, specialized prosecutors, secure evidence-management procedures, or institutional coordination. Comparative research on cybersecurity policy in developing countries demonstrates that legal reform must be accompanied by technical and administrative capacity if states are to respond effectively to sophisticated digital threats (18). This is especially relevant to Iraq, where post-conflict institution-building and cybersecurity capacity have developed under difficult political and economic conditions (7). Emerging technologies add further complexity. Assessments of technological readiness in Iraq indicate broader challenges associated with institutional adaptation to advanced digital systems, including artificial intelligence (19). Such developments are significant for cyberterrorism because artificial intelligence can strengthen both defensive cybersecurity tools and malicious operations.

Against this background, the central problem examined in this study is the extent to which Iraqi and Iranian legislation adequately identifies, criminalizes, investigates, and punishes terrorist crimes committed through cyberspace. The study focuses specifically on those cyber activities that possess a demonstrable terrorist purpose or relationship and excludes ordinary cyber offenses that lack such a connection. It examines the major forms of

terrorist conduct in cyberspace, including propaganda and recruitment, terrorist communication and coordination, cyber threats, electronic espionage, terrorist financing, attacks against data and information systems, and interference with critical infrastructure. It then evaluates the legislative response of Iraq and Iran, identifies common and distinctive legal gaps, and considers the principal directions in which their legal frameworks should develop. The objective of the study is to provide a comparative legal analysis of the principal forms of cyberterrorist crime and to assess the adequacy and development of Iraqi and Iranian legislation in confronting them.

### **Conceptual Framework and Types of Terrorist Crimes in Cyberspace**

The legal classification of terrorist crimes in cyberspace begins with the recognition that cyberspace can perform more than one role in the commission of terrorism. It may constitute the environment in which the offense occurs, the instrument through which a conventional terrorist objective is pursued, the target of the attack itself, or a support infrastructure facilitating terrorist activity elsewhere. This functional diversity makes a narrow technological definition inadequate. If cyberterrorism were limited only to destructive attacks against computer systems, a large range of digital terrorist conduct involving recruitment, propaganda, financing, intelligence collection, coordination, and intimidation would fall outside the concept. Conversely, defining every internet-related activity associated with extremist discourse as cyberterrorism would risk excessive criminalization. The more appropriate approach is therefore to examine the relationship between the digital conduct and the terrorist purpose pursued through it. Scholarship on internet-facilitated extremism has emphasized that the internet may contribute differently to radicalization, networking, mobilization, and operational activity, requiring careful differentiation among these functions (1). The Middle Eastern experience confirms that digital platforms have become integral to terrorist organizational strategies rather than merely supplementary communication devices (4).

One of the most important categories of cyberterrorist conduct consists of the dissemination and exchange of terrorist information. Terrorist organizations require communication systems through which members, supporters, recruiters, propagandists, financiers, and operational planners can exchange information. Digital networks dramatically reduce the cost and risk associated with such communication. Messages can be distributed across national borders within seconds, groups can reorganize after accounts or websites are removed, and communication may occur through public platforms, private messaging systems, encrypted applications, temporary accounts, or other forms of digital infrastructure. The terrorist use of communication technology was especially evident in the online practices of ISIS, whose digital strategy involved the dissemination of propaganda and the creation of a transnational network of supporters (2). Such conduct becomes legally significant when digital communication is intentionally used to facilitate terrorist membership, provide operational instructions, coordinate activities, conceal participants, or maintain organizational command structures.

The dissemination of extremist propaganda constitutes a related but distinct form of cyberterrorist activity. Digital propaganda can glorify terrorist violence, justify attacks through ideological or political narratives, celebrate perpetrators, delegitimize targeted communities or governments, and create social environments in which extremist conduct becomes normalized. Terrorist groups can reach audiences without controlling conventional broadcasting infrastructure and can adjust their messages for specific linguistic, religious, cultural, or demographic audiences. Hassan's examination of terrorist internet use demonstrates that online communication can function as an important ideological instrument for organizations seeking to spread extremist interpretations and sustain virtual networks of supporters (17). The legal challenge is to distinguish between prohibited terrorist propaganda and expression that

is controversial, radical, or politically offensive but does not meet the threshold for criminal responsibility. This requires attention to intent, context, the nature of the content, the relationship of the speaker to terrorist activity, and whether the communication directly encourages, assists, or facilitates terrorism.

Online recruitment is another major manifestation of cyberterrorism. Traditional terrorist recruitment often depended on physical meetings, personal networks, religious or political organizations, or direct contact with existing members. Digital platforms allow recruiters to identify individuals who express frustration, ideological sympathy, social isolation, or interest in extremist content and gradually move them toward more private forms of communication. Recruitment may involve ideological persuasion, emotional manipulation, promises of belonging or status, exposure to graphic propaganda, and eventual encouragement to provide material support or participate in terrorist operations. Analysis of internet use by violent extremist movements has shown that online environments can facilitate access to extremist networks even though digital exposure alone cannot explain the complex process of radicalization (1). Criminal legislation must therefore focus on purposeful recruitment and facilitation rather than assuming that mere access to extremist content proves terrorist intent.

The creation and management of terrorist websites, channels, and other digital platforms may similarly constitute a specific form of terrorist support. A website may operate as a virtual headquarters by publishing official statements, ideological texts, recruitment materials, training instructions, fundraising requests, operational claims, or communications directed to supporters. Modern platforms have expanded this model beyond conventional websites by allowing terrorist networks to migrate among social media accounts, encrypted messaging channels, file-sharing systems, and decentralized services. The resilience of such networks creates significant enforcement difficulties because a platform removed in one location may reappear through mirrors, new accounts, foreign hosting providers, or redistributed content. The experience of extremist organizations in the Middle East demonstrates that the internet can support decentralized communication and propaganda structures capable of surviving repeated disruption (3). Legal rules must therefore address intentional administration and facilitation of terrorist digital infrastructure while avoiding the imposition of liability on ordinary service providers that lack knowledge or criminal intent.

Cyberterrorist activity may also involve intelligence gathering. The open nature of the internet provides access to vast quantities of information concerning government institutions, public infrastructure, transportation systems, corporate facilities, security practices, maps, personnel, and technical systems. Some information may be openly available, while other information is obtained through unauthorized access, deception, malware, or electronic surveillance. When terrorist actors gather such information in preparation for attacks, target selection, surveillance, or operational planning, the conduct may become part of a terrorist offense even before physical violence occurs. The distinction between ordinary information gathering and punishable terrorist preparation depends on evidence of intent and connection to a terrorist plan. This issue becomes more serious when the conduct involves electronic espionage, because unauthorized interception or extraction of confidential governmental, military, or infrastructural information can directly endanger national security. The regional cybersecurity environment has demonstrated persistent threats involving espionage and unauthorized acquisition of sensitive information (16).

Electronic espionage in the cyberterrorist context includes the deliberate use of digital means to access, intercept, copy, or transmit protected information for terrorist purposes. Malware, phishing, compromised accounts, unauthorized network access, spyware, and remote-access tools may enable perpetrators to collect intelligence without entering the physical premises of the targeted institution. Such activity differs from traditional espionage because the offender may operate remotely, automate data collection, access numerous systems simultaneously,

and conceal activity through international digital infrastructure. The resulting information may be used to identify vulnerabilities, select attack targets, expose security personnel, interfere with governmental decision-making, or support hostile operations. Because espionage may also be conducted by states, criminal organizations, commercial actors, or individual hackers, terrorist intent again becomes the decisive legal factor. A coherent statutory system should therefore enable prosecutors to combine cybercrime provisions prohibiting unauthorized access or interception with terrorism provisions where the conduct is demonstrably linked to terrorist objectives.

Cyber threats and digital intimidation constitute another category. Terrorism has traditionally relied on the psychological effect of violence as well as the physical harm caused by attacks. Cyberspace greatly increases the ability to disseminate threats to large audiences, target specific public officials, threaten critical facilities, circulate fabricated attack announcements, or publish disturbing material designed to create panic. A threat transmitted digitally may have an immediate transnational audience and can be amplified through social media even where the perpetrator lacks the immediate capability to execute the threatened act. Terrorist intimidation may include threats to conduct bombings, attacks against public infrastructure, assassinations, cyber sabotage, or coordinated violence. It may also involve threats to release sensitive information, interfere with essential systems, or expose confidential data. The legal significance of such conduct lies in the deliberate creation of fear for a political or ideological purpose rather than the communication method alone. Regional studies of cyberterrorism emphasize that psychological disruption and intimidation can form an important part of digitally enabled terrorist strategy (3).

Attacks against websites, networks, electronic data, and information systems form the most technologically direct category of cyberterrorist crime. Such attacks may involve unauthorized access, deletion or alteration of data, installation of malicious software, denial-of-service attacks, interference with communication systems, or destruction of digital infrastructure. The terrorist character of these acts depends on the purpose for which they are committed and the target chosen. A denial-of-service attack against a commercial website for financial extortion may constitute ordinary cybercrime, whereas the same technique used to disable emergency communications during a coordinated terrorist attack may form part of cyberterrorism. Middle Eastern cybersecurity research has emphasized that states face substantial vulnerabilities because both public institutions and strategically important private-sector entities depend increasingly on interconnected digital systems (15). The expansion of these dependencies increases the potential consequences of terrorist cyber operations.

Attacks directed against critical infrastructure deserve particular legal treatment because they can produce consequences comparable to conventional terrorist violence. Electricity, water, transportation, health services, communications, banking systems, energy production, and government administration increasingly depend on digital control systems. Interference with these systems may cause widespread disruption, financial losses, panic, or physical harm. A successful attack against a power grid, for example, may affect hospitals, transportation networks, public communications, and essential services simultaneously. This means that the protected legal interest extends beyond the integrity of a computer system to public safety and national security. Cybersecurity policy in developing states must therefore treat infrastructure protection as both a technical and a legal priority (18). Regional threat reporting has similarly shown that malware and network attacks can target strategically important sectors and create national-level security concerns (16).

Distributed denial-of-service attacks illustrate how relatively familiar cyber techniques can acquire terrorist significance. By overwhelming servers or networks with large volumes of traffic, perpetrators may temporarily disable governmental websites, communication services, financial institutions, or other systems. The direct

technical damage may be limited, but the strategic effect can become substantial when the attack is timed to coincide with political unrest, military operations, terrorist violence, or coordinated propaganda campaigns. Recent research concerning low-level cyberattacks in geopolitical conflict demonstrates that even technically unsophisticated operations may contribute to wider political campaigns by generating disruption, symbolic impact, and publicity (12). The increasing role of hacktivist actors further complicates classification because politically motivated cyber groups may act independently, in informal coordination with state or terrorist actors, or in response to broader conflicts (10). Criminal law must therefore evaluate purpose, coordination, organizational connection, and intended effects rather than relying exclusively on technical severity.

Cyberterrorist financing also requires attention. Terrorist organizations depend upon financial resources for recruitment, logistics, weapons, communications, travel, propaganda, and operational support. Digital financial systems can facilitate transfers, conceal the origin or destination of funds, allow small-scale contributions from geographically dispersed supporters, or enable fundraising campaigns disguised as legitimate activities. Although not every digital transfer connected to terrorism constitutes cyberterrorism in a narrow technical sense, the use of cyberspace to finance terrorist activity forms an essential part of the digital terrorist ecosystem. Iran's broader counter-terrorism legislation has increasingly addressed terrorist financing as an independent legal problem, reflecting the international emphasis placed on disrupting the economic foundations of terrorism (9). Digitalization makes enforcement more difficult because financial transactions may move rapidly across jurisdictions and involve multiple intermediaries.

Emerging technologies are widening the range of potential terrorist misuse. Artificial intelligence may assist in automated reconnaissance, production of persuasive propaganda, generation of fraudulent identities, social engineering, analysis of stolen information, or adaptation of malicious code. Recent commentary has specifically highlighted the capacity of artificial intelligence to accelerate cyber operations associated with Iranian actors (11). At the same time, digitally connected physical devices can become instruments of political violence or security disruption. Research examining attacks involving everyday electronic devices demonstrates how ordinary technologies may be implicated in highly unusual security operations (20). These developments reinforce the need for technology-neutral criminal legislation. Laws that define offenses by reference to a particular device, software type, or communication platform may quickly become obsolete. Instead, the law should define prohibited conduct according to unauthorized interference, harmful consequences, terrorist intention, protected interests, and participation in terrorist activity.

A legally coherent classification can therefore be built around several overlapping functions of cyberspace in terrorism. Cyberspace enables ideological dissemination, recruitment, communication, planning, training, financing, intelligence collection, intimidation, espionage, and direct attacks on information systems or critical infrastructure. These functions differ in the immediacy and severity of harm, and not every one should necessarily receive the same punishment. A system of criminalization should distinguish between preparatory or supportive conduct, direct incitement, operational facilitation, attempted attacks, completed attacks, and conduct causing death or major infrastructure destruction. At the same time, the borderless nature of cyberspace requires legislation capable of addressing conduct that occurs partly outside national territory. The interaction between domestic criminal law and international cooperation is therefore central to the effective suppression of cyberterrorism (13). International agreements can help establish common standards, facilitate evidence exchange, support extradition, and reduce safe havens for offenders (14).

The classification of cyberterrorist offenses should ultimately remain grounded in the principle of legality. Terrorism is a serious offense that often attracts exceptional investigative powers and severe penalties. Broad or ambiguous definitions can therefore create substantial risks for freedom of expression, privacy, political activity, and legitimate cybersecurity research. Cyberterrorism should not become a label automatically applied to every politically motivated cyber offense. The criminal law must identify a sufficiently clear terrorist purpose, specify the prohibited digital conduct, and establish appropriate mental elements. This precision is particularly important for Iraq and Iran because both legal systems must confront genuine national-security threats while also creating statutory frameworks capable of being applied consistently by investigators, prosecutors, and courts. The classification developed here provides the basis for evaluating whether the two countries' existing laws satisfy these requirements.

### **Legislative Framework for Combating Cyberterrorism in Iraqi Law**

The Iraqi legal response to cyberterrorism must be understood within the broader political and security context that followed the collapse of the previous state structure in 2003, the emergence of armed insurgencies, sectarian violence, the expansion of terrorist organizations, and the later territorial rise of ISIS. Under these circumstances, terrorism became one of the most urgent concerns of Iraqi criminal policy. Yet the principal laws adopted to address terrorism were developed largely in response to conventional violence rather than the technological transformation of terrorist activity. The rapid growth of internet access, social media, encrypted communication, online propaganda, and cyber operations created a mismatch between traditional counter-terrorism provisions and new forms of digitally mediated conduct. Studies of cybersecurity in Iraq describe this mismatch as part of a broader institutional problem involving fragmented regulation, technical limitations, and the absence of a fully developed cybersecurity ecosystem (5). Consequently, Iraqi authorities have often had to respond to cyberterrorism through a combination of general anti-terrorism law, criminal-law provisions, procedural rules, institutional powers, and proposed cybercrime legislation.

The Anti-Terrorism Law No. 13 of 2005 forms the central statutory foundation for Iraq's response to terrorist conduct. Its importance lies in establishing a broad legal framework for acts intended to disturb security, threaten national unity, endanger public institutions, or advance terrorist objectives. The law was enacted in a context dominated by physical attacks, bombings, armed organizations, assassinations, and insurgent violence. It therefore does not provide a sophisticated or autonomous concept of cyberterrorism. Nevertheless, the functional breadth of terrorism-related provisions may allow some cyber-enabled conduct to be prosecuted where prosecutors can demonstrate a sufficient connection to terrorist objectives. For example, digital communication used to organize attacks, internet-based recruitment for terrorist groups, or electronic activity directly supporting a terrorist operation may fall within broader concepts of participation, assistance, or facilitation. The problem is that applying conventional terrorism provisions to digital conduct creates uncertainty regarding the precise elements of liability. Al-Jaberi's assessment of Iraqi cybercrime regulation highlights the continuing need for legislative provisions that more directly address contemporary forms of digital criminal activity (6).

This uncertainty is particularly important under the principle of legality. Criminal offenses should be defined with enough clarity that individuals can determine what conduct is prohibited and courts can apply the law consistently. Where a general terrorism provision is extended to new forms of online conduct without clear statutory criteria, questions may arise concerning interpretation, proportionality, and the distinction between criminal terrorist support

and lawful digital expression. Iraq's legal system therefore requires a clearer framework specifying when online propaganda, recruitment, digital coordination, cyber threats, data interference, or attacks on information systems qualify as terrorist offenses. This does not necessarily require the creation of a completely separate code of cyberterrorism. A more coherent approach could combine general definitions of terrorism with specific cybercrime offenses and statutory aggravating or qualifying circumstances where those offenses are committed for terrorist purposes.

The Counter-Terrorism Agency Law No. 31 of 2016 represents an important institutional development because it provides the specialized counter-terrorism apparatus with powers relevant to contemporary terrorist threats. The agency's ability, subject to judicial authorization, to monitor communications, social media platforms, and websites reflects formal recognition that terrorist activity increasingly occurs within digital environments. This power is significant for investigations involving online recruitment, communication between terrorist cells, propaganda networks, or planning through electronic platforms. Yet surveillance authority alone does not solve the broader legal problem. Investigators must still identify the substantive offense, collect evidence in a legally admissible form, connect digital activity to particular persons, and demonstrate the required terrorist intent. Moreover, monitoring powers must be regulated by judicial and procedural safeguards to ensure that the exceptional nature of counter-terrorism does not eliminate basic protections for privacy and lawful communication.

The problem of electronic evidence is especially important in the Iraqi context. Cyberterrorism frequently leaves evidence in forms that differ fundamentally from traditional physical evidence. Relevant material may include server logs, social-media communications, metadata, IP information, stored messages, cloud-based files, digital financial records, encrypted devices, malware samples, forensic images, or data obtained from foreign service providers. The effectiveness of criminal prosecution therefore depends on clear rules governing seizure, preservation, authenticity, chain of custody, forensic examination, and courtroom admissibility. Traditional procedural frameworks may not adequately address these issues. Iraqi cybercrime scholarship has emphasized the importance of modernizing legal procedures alongside substantive criminalization (6). Without such modernization, investigators may successfully identify suspicious digital activity while prosecutors remain unable to present reliable evidence that satisfies judicial requirements.

Attribution creates an additional difficulty. The person controlling a terrorist account or launching a cyberattack may use false identities, compromised devices, proxy servers, virtual private networks, anonymization systems, or infrastructure located outside Iraq. The technical source of an electronic communication does not automatically establish the identity or intention of the perpetrator. Effective prosecution therefore requires specialized forensic expertise and cooperation with service providers and foreign authorities. Research on Iraqi cybersecurity capacity has noted the importance of specialized human resources, institutional training, and technical infrastructure (7). The legal system must consequently be supported by cyber forensic laboratories, trained investigative judges, prosecutors familiar with digital evidence, and procedures for rapid preservation of electronic information. Legal reform without this technical capacity would produce only limited practical change.

Extraterritoriality is another major weakness in traditional legal approaches to cyberterrorism. A terrorist cyber operation directed against Iraq may be launched entirely from outside Iraqi territory. The perpetrator may never enter the country, while the servers, communication platforms, and digital accounts involved in the offense may be distributed across several jurisdictions. Traditional territorial rules can therefore become inadequate. Cybersecurity and international law scholarship demonstrates that digitally mediated conduct creates complex jurisdictional

problems because territorial location is often difficult to define in a meaningful way (13). Iraqi law needs sufficiently clear jurisdictional rules permitting prosecution where cyberterrorist conduct produces substantial effects within Iraq, targets Iraqi critical infrastructure or governmental institutions, involves Iraqi victims, or is committed by persons subject to Iraqi jurisdiction. Such rules must then be complemented by extradition and mutual legal assistance arrangements.

International cooperation is particularly important because electronic evidence can disappear rapidly. A social-media account can be deleted, a server log overwritten, or data moved to another jurisdiction before a formal legal request is processed. Counter-cyberterrorism therefore requires mechanisms for urgent preservation requests, data sharing, coordinated investigations, and technical cooperation. Karamifar and colleagues emphasize the role of international legal arrangements in confronting the cross-border nature of cyberterrorism (14). Iraq's participation in regional legal instruments, including the Arab Convention on Combating Information Technology Crimes, provides an important basis for harmonization and cooperation. Nevertheless, treaty participation becomes effective only when domestic law provides the necessary substantive offenses, procedural powers, and institutional capacity required to implement international obligations.

The long-running debate surrounding Iraqi cybercrime legislation illustrates the difficulty of developing an appropriate regulatory framework. Cybercrime laws can be essential for defining unauthorized access, unlawful interception, data interference, system interference, electronic fraud, identity misuse, and other conduct that may form the technical component of cyberterrorist offenses. However, such laws can also create risks when provisions concerning public order, national security, or online expression are drafted in vague terms. The Iraqi legislative challenge is therefore not simply to enact a cybercrime statute but to ensure that the statute is technically precise, consistent with terrorism legislation, and compatible with procedural safeguards. Al-Dabbagh identifies shortcomings in Iraq's cybersecurity environment that cannot be solved exclusively through punitive legislation (5). Similarly, Mahmud argues that capacity building is essential in the post-conflict Iraqi context because the effective implementation of cybersecurity policy depends upon institutional competence (7).

The relationship between cyberterrorism and freedom of expression is particularly sensitive. Terrorist organizations use online platforms to disseminate propaganda and recruit supporters, but political, religious, and social discourse may also include radical, controversial, or sharply critical expression. A criminal provision that fails to distinguish between advocacy, extremist opinion, direct incitement, recruitment, and operational facilitation may enable arbitrary enforcement. Iraqi legislation should therefore define the threshold at which online content becomes punishable as terrorist activity. Relevant considerations may include intentional encouragement of terrorist acts, recruitment into prohibited organizations, dissemination of operational instructions with terrorist intent, direct coordination with terrorist entities, or provision of material assistance. Merely possessing controversial opinions or accessing information should not automatically establish terrorist liability. Precision is particularly important because counter-terrorism offenses often carry severe penalties.

The protection of critical infrastructure requires a further dimension of legislative reform. Iraq's energy, oil, transportation, telecommunications, banking, governmental, and security sectors increasingly depend upon digital infrastructure. Cyberattacks directed at such systems may create effects extending far beyond the immediate computer network. Regional studies indicate that Middle Eastern states face persistent difficulties in aligning cybersecurity capabilities with the rapidly expanding threat environment (15). Iraqi law should therefore recognize the increased gravity of cyber offenses targeting essential services when they are committed with terrorist intent.

This may involve aggravated penalties, specialized investigative procedures, mandatory security obligations for critical infrastructure operators, and mechanisms for immediate reporting of serious cyber incidents.

The emergence of artificial intelligence and advanced digital tools makes technological neutrality equally important. Iraq should avoid drafting criminal provisions around specific technologies because new methods of cyberattack and communication develop more quickly than legislative amendment. The broader issue of technological readiness has become increasingly important for Iraqi governance (19). A durable legislative framework should define offenses according to conduct and protected interests rather than specific platforms. Unauthorized interference with critical systems, terrorist exploitation of digital communication, intentional recruitment, digital financing, and cyber-enabled intimidation should remain punishable regardless of whether they are carried out through current social-media applications, future artificial intelligence systems, decentralized networks, or technologies not yet widely used.

Another weakness concerns institutional fragmentation. Cyberterrorism can involve national-security agencies, police, intelligence institutions, prosecutors, courts, communications regulators, cybersecurity bodies, financial authorities, and private internet or telecommunications companies. Without clear coordination mechanisms, the same case may fall between several institutions, evidence may not be shared effectively, and investigative responses may become delayed. Iraqi cybersecurity analysis repeatedly stresses the importance of institutional coordination (5). A national framework should therefore specify operational responsibilities, establish procedures for joint investigation, define channels for information exchange, and ensure that cybersecurity agencies can cooperate lawfully with criminal justice institutions.

The Iraqi legal system must also distinguish between terrorist cyber offenses and politically motivated but non-terrorist cyber conduct. Recent international experience shows that hacktivist groups may engage in website disruption, data leaks, and denial-of-service attacks during geopolitical conflicts (10). Such acts can be unlawful and serious without necessarily satisfying the legal definition of terrorism. Likewise, research on low-level cyberattacks demonstrates that many politically motivated operations generate disruption without producing the scale of fear, violence, or coercive effects traditionally associated with terrorism (12). Iraqi law should therefore avoid equating every cyberattack against the state with terrorism. The terrorist designation should require additional elements relating to purpose, intended intimidation, coercion, organizational connection, or serious threat to public security.

The development of Iraqi legislation should accordingly proceed through integration rather than isolated statutory expansion. General anti-terrorism rules must be connected systematically with cybercrime offenses, criminal procedure, electronic evidence, cybersecurity regulation, and international cooperation. The central deficiency is not that Iraqi law completely ignores digital terrorism but that the relevant provisions are fragmented and not always adapted to the technological characteristics of cyber offenses. A coherent model would expressly recognize cyber-enabled terrorist conduct, define the relationship between terrorist intent and underlying computer offenses, regulate digital investigation and evidence, establish extraterritorial jurisdiction for serious attacks affecting Iraq, provide special protection for critical infrastructure, and strengthen institutional capacity. Such development would move Iraqi criminal policy from reactive application of conventional terrorism law toward a more comprehensive framework capable of responding to contemporary cyberterrorism.

## Iranian Legislation and Comparative Evaluation of the Iraqi and Iranian Approaches

Iran's legal response to cyberterrorism has developed through a combination of computer-crime legislation, national-security provisions, terrorism-related rules, terrorist-financing legislation, and specialized institutional mechanisms. Compared with Iraq, Iran has established a more developed statutory framework for computer offenses, particularly through the Computer Crimes Law adopted in 2009. This legislation provides a legal basis for addressing conduct such as unauthorized access, interception, data-related offenses, interference with computer systems, and other forms of digital misconduct. It therefore supplies many of the underlying offenses that may form the technical component of cyberterrorism. Ghafarian and Shahi describe Iran's cybersecurity framework as an important development while also identifying legal challenges resulting from the continuing evolution of digital threats (8). The key analytical issue is that a computer offense and a terrorist offense are conceptually distinct. Iranian law may criminalize unauthorized access or system interference without necessarily defining when such conduct should be legally characterized as cyberterrorism.

The Computer Crimes Law is significant because cyberterrorist attacks frequently depend on acts that are already recognized as computer offenses. A terrorist group seeking to disable government infrastructure may first gain unauthorized access to a network, install malicious software, extract protected data, interfere with system functions, or destroy information. These technical acts can be prosecuted under cybercrime provisions, while their terrorist purpose may engage separate national-security or terrorism-related rules. This layered approach can provide flexibility, but it can also create uncertainty if legislation does not clearly specify how the offenses interact. The absence of a unified definition of cyberterrorism may lead prosecutors to rely on different legal categories depending on the facts of each case, creating potential inconsistencies in charging and sentencing. The Iranian framework therefore demonstrates both the advantages and limitations of using specialized cybercrime legislation alongside broader security law (8).

Iran's approach to terrorism itself has historically differed from systems that enacted comprehensive terrorism codes. Various forms of politically or ideologically motivated violence have been addressed through existing criminal concepts and national-security offenses. Over time, however, increasing international attention to terrorism financing contributed to the development of more explicit statutory rules. Iran's Anti-Terrorism Financing Law represents an important stage in this evolution because it directly addresses the economic support of terrorist conduct. Akbarzadeh's analysis of Iran's position in the global struggle against terrorism illustrates the distinctive political and legal context in which Iranian counter-terrorism policy developed (9). Terrorist financing is especially relevant to cyberspace because digital platforms and financial technologies can support fundraising, transfer of resources, concealment of beneficiaries, and cross-border transactions associated with terrorist organizations.

The relationship between terrorist financing and cyberterrorism demonstrates why modern legislation must regulate supportive conduct as well as completed attacks. Terrorist operations require financial and logistical structures that may be maintained partly through digital systems. Online fundraising campaigns, electronic payment mechanisms, false charitable appeals, or concealed transfers can contribute to terrorist activity without themselves causing physical destruction. A comprehensive criminal policy should therefore address digital financial support when the requisite knowledge and terrorist purpose are established. International cooperation becomes essential because electronic financial transactions may pass through several jurisdictions and service providers. The broader international-law literature on cybersecurity emphasizes the increasing importance of transnational cooperation in

addressing digitally mediated threats (13), while research on treaties relating specifically to cyberterrorism highlights the need for mechanisms that enable states to coordinate investigation and prosecution (14).

The Iranian cybersecurity experience is also inseparable from the country's exposure to major cyber operations affecting strategic sectors. Cyberattacks directed against Iranian industrial, energy, governmental, and financial systems have demonstrated the national-security consequences of digital vulnerabilities. Although not every attack against Iranian infrastructure constitutes terrorism, such incidents have contributed to the development of legal and institutional concern regarding cyber defense. Threat reporting across the Middle East shows that malicious software, espionage, data theft, and infrastructure attacks have become persistent elements of the regional security landscape (16). This experience has encouraged Iran to treat cyber capabilities as an important component of national security. Yet legal classification remains complicated because an operation may constitute espionage, sabotage, cyber warfare, politically motivated cybercrime, or terrorism depending upon the actor, purpose, target, and consequences.

The distinction is increasingly significant in contemporary geopolitical conflict. Recent scholarship indicates that relatively low-level cyber operations may accompany military and political confrontation without necessarily reaching the threshold of terrorism or armed attack (12). Hacktivist activity further complicates attribution because non-state groups may conduct politically motivated operations that appear aligned with state objectives but lack formal command structures (10). Iranian law, like Iraqi law, therefore requires criteria capable of distinguishing cyberterrorism from other politically motivated cyber activity. Treating every hostile cyber operation as terrorism would conceptually expand terrorism beyond useful legal limits and could obscure the differences among national-security crimes, espionage, sabotage, and terrorist violence.

Iran's legislative framework must also respond to the use of cyberspace for terrorist communication, propaganda, and recruitment. The technical provisions of computer-crime law do not necessarily address these activities because the offender may use digital systems lawfully from a technical perspective while pursuing an unlawful terrorist purpose. A person who creates an online recruitment channel, distributes terrorist propaganda, or communicates instructions through an ordinary messaging service may not engage in unauthorized access or system interference. Liability therefore depends on terrorism, incitement, participation, or national-security provisions rather than conventional computer offenses. The literature on online violent extremism demonstrates that terrorist use of the internet extends far beyond hacking (1). Hassan similarly shows that digital platforms can become ideological and organizational environments for extremist networks (17). Iranian legislation consequently requires a clear connection between general counter-terrorism rules and online conduct.

The protection of critical infrastructure is another area in which Iran's experience provides an important comparative perspective. The country's strategic dependence on energy, industrial, financial, communications, and governmental networks creates strong incentives for the development of cybersecurity capabilities. From a criminal-law perspective, cyberattacks against such systems should be assessed according to both the technical interference involved and the terrorist objective. Where the purpose is to intimidate the population, compel state action, destabilize public order, or support a terrorist campaign, the act should be treated more severely than ordinary system interference. Regional cybersecurity studies emphasize that infrastructure vulnerability is one of the most serious challenges confronting Middle Eastern states (15). Effective legislation should therefore permit differentiated punishment according to the importance of the target, the scale of disruption, the creation of danger to human life, and the terrorist purpose of the offender.

Electronic evidence is crucial in Iranian cyberterrorism cases for the same reasons that it is important in Iraq. Terrorist communication, digital financing, network intrusion, and online propaganda all generate evidence in electronic form. Iran's more developed cybercrime framework provides a stronger legal environment for specialized digital investigations, but continuing technological change creates new evidentiary challenges. Encryption, cloud computing, anonymous communication services, foreign-hosted platforms, artificial intelligence-generated content, and decentralized technologies can complicate identification and attribution. The evidentiary problem becomes particularly serious when the prosecution must prove terrorist intent in addition to establishing the underlying digital act. An unauthorized access offense may be technically demonstrable, yet characterization as cyberterrorism requires evidence concerning motive, organizational relationships, communications, target selection, or broader operational planning.

Artificial intelligence represents a rapidly emerging challenge for the Iranian framework. Recent analysis suggests that AI can accelerate cyber operations associated with Iranian actors by assisting information analysis, social engineering, content production, and other operational tasks (11). Regardless of the identity of the actor using the technology, this development has broader implications for cyberterrorism legislation. AI-generated propaganda may be produced at large scale, malicious code may be adapted more rapidly, and deceptive communications can become more persuasive. The appropriate legislative response is not to criminalize artificial intelligence itself but to ensure that existing offenses remain applicable when AI is used as the instrument of terrorist conduct. Technology-neutral drafting is therefore essential.

The comparison between Iraq and Iran reveals an important difference in the maturity of their digital legal frameworks. Iraq's counter-terrorism legislation is strong in its general focus on terrorist violence and national security but remains comparatively fragmented in relation to specialized cybercrime regulation. Iran possesses a more established computer-crime framework that directly criminalizes many forms of unauthorized digital conduct. This gives Iranian authorities a clearer statutory basis for prosecuting the technical components of cyberterrorist operations. The distinction corresponds with wider assessments of cybersecurity capacity in the region, where states vary considerably in legal development, institutional specialization, and technical resources (18). Iraq's post-conflict circumstances have made capacity building particularly difficult (7), while Iran's longer institutional engagement with cybersecurity has produced a comparatively more structured approach (8).

Nevertheless, neither system fully resolves the conceptual problem of cyberterrorism. Both rely to varying degrees on combining terrorism-related offenses with cybercrime or national-security provisions. This can be legally workable, but only if the relationship between the different categories is sufficiently clear. The central requirement is not necessarily the adoption of a single offense entitled "cyberterrorism." Instead, legislation should clarify when a cyber offense becomes terrorist in nature, what additional mental element is required, what consequences justify aggravated punishment, and how participation or assistance is treated. A precise definition should avoid both under-criminalization and over-criminalization. If the definition is too narrow, terrorist actors may exploit gaps between traditional terrorism and cybercrime statutes. If it is too broad, ordinary hacking, political protest, or controversial online expression may be inappropriately characterized as terrorism.

A second comparative issue concerns jurisdiction. Both Iraq and Iran face cyber threats that may originate abroad. Territorial criminal law is insufficient when perpetrators, infrastructure, victims, and consequences are distributed among several states. Fidler's analysis of cybersecurity under international law demonstrates the difficulty of applying conventional concepts of sovereignty and jurisdiction to cross-border cyber operations (13).

Both countries therefore require clear rules allowing jurisdiction over attacks directed against their governmental systems, critical infrastructure, national security, or citizens even when the offender acts outside national territory. At the same time, such jurisdiction must be supported by realistic international cooperation. Legal authority to prosecute has limited value where the suspect, evidence, or relevant service provider is located in a state unwilling or unable to cooperate.

A third comparative issue is electronic evidence. Iraq faces particularly significant procedural and technical difficulties, while Iran's more specialized cybercrime system provides a stronger foundation. Nevertheless, both systems must continually update evidentiary procedures because digital evidence changes rapidly. Rules should address preservation, seizure, forensic imaging, authentication, metadata, integrity, chain of custody, and the treatment of evidence obtained from foreign providers. Investigative agencies should also possess the capacity to distinguish manipulated or artificial content from authentic evidence. The increasing accessibility of sophisticated digital tools means that the evidentiary environment will become more difficult rather than simpler.

A fourth issue concerns institutional capacity. Laws against cyberterrorism are ineffective without specialized personnel and coordinated agencies. Iraq has a particularly strong need for capacity building, as emphasized in research on its post-conflict cybersecurity development (7). Iran also requires continuing institutional adaptation because the threat environment is evolving rapidly. Both countries should strengthen cooperation among law-enforcement agencies, intelligence bodies, prosecutors, judicial authorities, communications regulators, financial institutions, cybersecurity agencies, and critical-infrastructure operators. Training should include digital forensics, cyber attribution, malware analysis, financial tracing, international evidence requests, and legal evaluation of terrorist intent.

A fifth comparative issue concerns international cooperation. Cyberterrorism is inherently transnational, and neither Iraq nor Iran can address it exclusively through domestic law. International treaties and regional agreements can harmonize criminal definitions, provide mutual legal assistance, facilitate extradition, and establish channels for urgent evidence preservation (14). Yet international cooperation must account for political realities, differing legal systems, and questions of sovereignty. Both countries should therefore pursue practical arrangements that enable technical cooperation and criminal investigation while maintaining appropriate legal safeguards.

A sixth issue concerns fundamental rights. Counter-terrorism and cybersecurity legislation can create strong incentives for expanded surveillance and restrictions on online communication. Yet not every controversial or oppositional statement constitutes terrorism. Both Iraqi and Iranian legislation should distinguish clearly between direct terrorist recruitment, incitement, operational support, and lawful expression. This requires precise statutory language and meaningful judicial oversight of intrusive investigative powers. The goal of countering terrorist exploitation of cyberspace should not become a justification for unlimited monitoring or ambiguous criminalization.

Finally, both legal systems need anticipatory rather than purely reactive legislation. The emergence of AI-assisted cyber operations (11), evolving hacktivist networks (10), digitally connected devices capable of being incorporated into security operations (20), and rapidly changing geopolitical cyber activity (12) demonstrate that legislation tied to existing technologies will quickly become outdated. The most effective comparative direction is therefore to formulate technology-neutral offenses based on protected interests, prohibited conduct, terrorist intent, and harmful consequences. Iraq can benefit from developing a more integrated cybercrime and electronic-evidence framework, while Iran can improve the connection between its existing computer-crime legislation and explicit rules concerning terrorist purpose. Both systems should strengthen critical-infrastructure protection, international cooperation,

jurisdictional rules, evidentiary procedures, institutional specialization, and safeguards against excessive criminalization. Such reforms would move the legal response from fragmented adaptation toward a coherent model of cyberterrorism regulation.

## Conclusion

The transformation of terrorism through digital technologies has created a category of criminal conduct that cannot be adequately addressed through conventional terrorism law or ordinary cybercrime legislation in isolation. Terrorist actors can now exploit cyberspace at nearly every stage of their activities, including ideological dissemination, recruitment, communication, intelligence gathering, operational planning, intimidation, financing, espionage, and direct attacks against information systems and critical infrastructure. The defining characteristic of cyberterrorism is therefore not the mere use of a computer or the internet but the relationship between digital conduct and a terrorist objective. The same technological act may constitute ordinary cybercrime in one context and a terrorist offense in another depending on its purpose, target, intended consequences, and connection to terrorist organizations or operations. Any coherent criminal policy must preserve this distinction.

The analysis demonstrates that cyberterrorist crimes should be understood as a functionally diverse group of offenses rather than a single technical form of attack. Some offenses use cyberspace primarily as a communication environment, as in terrorist propaganda, recruitment, ideological mobilization, and coordination. Others use digital technology as an investigative or preparatory instrument, including intelligence gathering, surveillance, and electronic espionage. A further category involves the use of cyberspace to intimidate populations or public authorities through threats and psychological operations. The most technically direct category consists of cyberattacks against data, networks, government systems, communications, and critical infrastructure. Terrorist financing may also increasingly occur through digital channels. These forms of conduct differ substantially in seriousness and proximity to physical harm, which means that legislation should differentiate among preparatory activity, facilitation, direct participation, attempted attack, completed attack, and conduct producing serious physical or infrastructural consequences.

The Iraqi legal framework has developed primarily from the country's urgent need to confront severe terrorism and insecurity. The Anti-Terrorism Law No. 13 of 2005 remains the central foundation of Iraqi counter-terrorism law, while the Counter-Terrorism Agency Law No. 31 of 2016 provides important institutional powers relevant to monitoring digital communications and online terrorist activity. Nevertheless, these instruments were not designed as comprehensive responses to cyberterrorism. The principal weakness of the Iraqi approach is therefore fragmentation. Terrorism law, criminal procedure, proposed cybercrime regulation, communications monitoring, and electronic evidence do not yet operate as parts of a completely integrated statutory framework. This fragmentation becomes especially problematic where an offense is committed remotely, involves foreign digital infrastructure, requires electronic evidence, or consists of online support rather than conventional terrorist violence.

Iraq consequently requires a more explicit legislative connection between terrorism and cybercrime. The adoption and refinement of modern cybercrime legislation should not merely create a broad catalogue of internet offenses. It should define core forms of unauthorized access, interception, data interference, system interference, digital threats, and other technologically specific conduct with sufficient precision, while allowing those offenses to receive an aggravated legal characterization when committed for terrorist purposes. Terrorist purpose should itself be clearly defined through elements such as deliberate intimidation of a population, coercion of public authorities,

serious destabilization of state institutions, or intentional support for a recognized terrorist organization. This approach would reduce uncertainty while avoiding the unnecessary expansion of terrorism law to ordinary cybercrime.

Electronic evidence represents one of the most important priorities for Iraqi reform. Cyberterrorism investigations depend heavily on data whose evidentiary characteristics differ from conventional physical evidence. Iraqi legislation should establish clear procedures for the lawful preservation, seizure, extraction, forensic analysis, authentication, transfer, and presentation of electronic evidence. Courts should be equipped to evaluate the reliability of digital forensic methods, and investigators should follow standardized chain-of-custody procedures. Specialized training for judges, prosecutors, investigators, and forensic experts is necessary because technological evidence cannot be managed effectively through statutory reform alone.

The Iranian legal framework is comparatively more developed in relation to computer offenses. The Computer Crimes Law provides a clearer statutory basis for prosecuting unauthorized access, interception, data interference, and other conduct that may form the technical foundation of a cyberterrorist attack. Iran has also developed legislation concerning terrorist financing and has created more specialized cybersecurity institutions. These features give the Iranian framework greater structural capacity to address the digital components of terrorist operations. Nevertheless, the Iranian system shares an important problem with Iraq: the relationship between cybercrime and terrorism is not always articulated through a unified and precise legal framework.

Iran should therefore clarify when offenses under computer-crime legislation acquire a specifically terrorist character. Unauthorized access, malware deployment, system disruption, or data destruction should not automatically be classified as terrorism simply because the target is politically sensitive. The classification should depend on a demonstrable terrorist purpose and an intention to produce consequences such as public intimidation, coercion of the government, serious destabilization, or facilitation of terrorist activity. Greater clarity in this area would improve consistency in prosecution and preserve the conceptual distinction among terrorism, cyber espionage, sabotage, hacktivism, cyber warfare, and politically motivated cybercrime.

The comparison of the two systems shows that Iraq's principal need is the development of a coherent and technically modern cybercrime and electronic-evidence framework, while Iran's principal need is greater integration between its existing cybercrime rules and its terrorism-related criminal policy. Despite this difference, both legal systems face common problems concerning attribution, jurisdiction, cross-border evidence, technological change, critical infrastructure, international cooperation, and the protection of fundamental rights. These common challenges provide a strong basis for parallel legal development even where the substantive structures of Iraqi and Iranian criminal law remain different.

Jurisdiction should be one of the central areas of reform in both states. Cyberterrorist offenses frequently lack a single identifiable crime scene. The perpetrator may operate abroad, the relevant server may be located in another country, and the harmful effects may occur within Iraq or Iran. Both states should therefore recognize jurisdiction over serious cyberterrorist conduct directed against their national security, public institutions, critical infrastructure, or citizens even when substantial parts of the conduct occur outside national territory. At the same time, extraterritorial jurisdiction should be exercised consistently with international law and supported through mechanisms of international criminal cooperation.

Critical infrastructure also deserves specific protection. Modern states depend on digital systems for electricity, water, transportation, health care, financial services, telecommunications, defense, and public administration. A

terrorist cyberattack against such infrastructure may cause consequences far exceeding the direct damage to a computer system. Both Iraq and Iran should establish heightened criminal liability where cyberterrorist conduct intentionally targets essential services or creates serious danger to life, national security, or economic stability. Critical-infrastructure operators should also be subject to cybersecurity, incident-reporting, and cooperation requirements that enable state institutions to respond rapidly to major threats.

International cooperation is indispensable. Terrorist networks and digital infrastructure do not respect territorial boundaries, and unilateral investigation frequently becomes impossible when evidence or suspects are located abroad. Iraq and Iran should strengthen mechanisms for mutual legal assistance, preservation of electronic evidence, exchange of technical information, coordinated investigation, extradition where legally available, and cooperation with regional and international cybersecurity institutions. Such cooperation is particularly important because the value of digital evidence can decline rapidly if preservation measures are delayed.

Institutional development should accompany legislative reform. Specialized cyberterrorism units should bring together technical investigators, counter-terrorism specialists, financial investigators, prosecutors, and digital forensic experts. Judges and prosecutors should receive sustained training in the technical characteristics of cyber offenses, while cybersecurity personnel should understand the evidentiary and procedural standards required in criminal cases. Coordination among intelligence services, law-enforcement agencies, financial regulators, telecommunications bodies, and critical-infrastructure operators should be formalized through clear legal procedures rather than depending on ad hoc cooperation.

Both countries must also ensure that cyberterrorism laws remain compatible with the principle of legality and do not become excessively broad instruments for regulating online expression. Terrorist propaganda, recruitment, incitement, and operational support are legitimate subjects of criminal prohibition when defined precisely, but controversial political speech or access to information should not automatically produce terrorism liability. Judicial authorization and proportionality should govern intrusive surveillance powers, and criminal responsibility should depend on proof of the required mental element. These safeguards are essential not only for protecting rights but also for preserving the credibility and effectiveness of counter-terrorism law.

Future legislation should be technology-neutral. Artificial intelligence, decentralized communication networks, advanced encryption, autonomous systems, synthetic media, and digitally connected devices will continue to alter the technological environment in which terrorist and counter-terrorist activities occur. Criminal statutes should therefore avoid definitions tied narrowly to specific devices or platforms. The focus should remain on unauthorized conduct, protected interests, terrorist intent, participation, consequences, and the seriousness of the threat. This approach enables the law to respond to technological evolution without requiring constant reconstruction of the basic criminal framework.

Ultimately, the most effective legal response to cyberterrorism in Iraq and Iran requires integration rather than the continuous accumulation of isolated offenses. Counter-terrorism law, cybercrime legislation, electronic-evidence rules, cybersecurity policy, terrorist-financing regulation, critical-infrastructure protection, and international cooperation should operate as interconnected components of a unified criminal policy. Iraq must overcome legislative fragmentation and strengthen technical and institutional capacity, while Iran should improve the precision with which its more developed cybercrime framework interacts with terrorism legislation. In both states, effective reform requires a balance between security and legality. Cyberterrorism is dynamic, transnational, and

technologically adaptable, but the law must remain precise, proportionate, enforceable, and capable of protecting both national security and the fundamental principles upon which legitimate criminal justice depends.

### Acknowledgments

We would like to express our appreciation and gratitude to all those who helped us carrying out this study.

### Authors' Contributions

All authors equally contributed to this study.

### Declaration of Interest

The authors of this article declared no conflict of interest.

### Ethical Considerations

All ethical principles were adhered in conducting and writing this article.

### Transparency of Data

In accordance with the principles of transparency and open research, we declare that all data and materials used in this study are available upon request.

### Funding

This research was carried out independently with personal funding and without the financial support of any governmental or private institution or organization.

### References

1. Conway M. Determining the role of the internet in violent extremism and terrorism: Six suggestions for progressing research. *Studies in Conflict & Terrorism*. 2017;40(1):77-98. doi: 10.1080/1057610X.2016.1157408.
2. Al-Rawi A. Cyberterrorism in the Middle East: The case of ISIS. *Journal of Strategic Security*. 2017;10(1):1-17. doi: 10.5038/1944-0472.10.1.1547.
3. Al-Kaabi FA, Al-Kahtani MA. Cyber terrorism: Threats and responses in the Middle East. *Journal of Security Studies*. 2018;12(3):210-25.
4. Efrati N, Kshetri N. Cybercrime and cyberterrorism in the Middle East: A comprehensive review. *Journal of Global Security Studies*. 2021;6(2):ogab004.
5. Al-Dabbagh M. Cybersecurity challenges in Iraq: An overview. *Journal of Information Security and Cybercrimes Research*. 2020;3(1):1-10. doi: 10.26735/iszv5079.
6. Al-Jaberi R. Digital security and cybercrime legislation in Iraq: A critical analysis. *Iraqi Journal of Information and Communication Technology*. 2022;4(2):35-50.
7. Mahmud AH. Cybersecurity capacity building in post-conflict Iraq: Challenges and opportunities. *International Journal of Cyber Policy*. 2022;5(3):201-15.
8. Ghafarian M, Shahi A. The legal framework for cybersecurity in Iran: An analysis of current challenges. *Iranian Journal of Legal Studies*. 2020;6(2):55-70.
9. Akbarzadeh S. Iran and the Global War on Terror: Challenges and Responses. *Middle East Policy*. 2015;22(1):98-109. doi: 10.1111/mepo.12118.
10. Le M. The new era of hacktivism. 2024 2024/10/23.
11. Lawfare. Artificial intelligence is accelerating Iranian cyber operations. *Lawfare*. 2024.

12. Vu AV, Hutchings A, Anderson R. Yet another diminishing spark: Low level cyberattacks in the Israel Gaza conflict. [Preprint]. In press 2025.
13. Fidler D. Cybersecurity and international law. *Indiana Journal of Global Legal Studies*. 2015;21(2):317-36.
14. Karamifar F, Tabibian S, Rezaei SA. The role of international treaties in combating cyber terrorism: A legal analysis. *Legal Studies in the Digital Age*. 2024.
15. Benton M, Atkinson RD. Cybersecurity in the Middle East: Bridging the gap between threats and capabilities. *Journal of Cyber Policy*. 2016;1(2):207-23. doi: 10.1080/23738871.2016.1238953.
16. Kaspersky L. Cyberthreats in the Middle East: Trends and statistics. 2020.
17. Hassan H. The cyber jihad: How terrorists use the internet. *Journal of Terrorism Research*. 2019;10(2):25-38. doi: 10.15664/jtr.1477.
18. Cruz TJ, Simoes P. Cybersecurity in developing countries: Threats and policy responses. *Computers & Security*. 2019;87:101581. doi: 10.1016/j.cose.2019.101581.
19. Alalaq AS. The Oxford Insights Government AI Readiness Index: A case study of Iraq. [Preprint]. In press 2025.
20. Sarker PP, Das U, Varshney N, Shi S, Kulkarni A, Farahmandi F, et al. When everyday devices become weapons: A closer look at the pager and walkie talkie attacks. [Preprint]. In press 2025.