Digital Terrorism as an Emerging Threat to Cybersecurity

Dr: Aicha Merdjal

Institute of Law

Law Department

Governance Horizons Laboratory for Sustainable Local Development

University Center of Barika / Algeria

Dr: Nadia Kadri

Institute of Law

Law Department Governance Horizons Laboratory for Sustainable Local Development

University Center of Barika / Algeria

Submission Date: 29 Jun 2025 **Approval Date:** 29 Aug 2025 **Release Date:** 29 Sep 2025

Abstract

As a result of technological development, the international community's shift towards the adoption of digital technology in various international transactions this way, the electronic network and technological means have become fundamental necessities that underscore the power of the State in the international arena, where all States have digitally stored their basic data excluding the traditional paper system, This has contributed to the emergence of emerging threats to international peace and security that affect the State's internal stability.

As a reflection of the digital development of the international community, emerging crimes have emerged in the international arena that depend in their attacks on the digital dynamics of the State's electronic infrastructure and work to attack and destroy them.

Among them is cyber terrorism, a transformative extension of traditional terrorism, which has become one of the most difficult challenges facing the international community.

This paper is therefore interested in studying the topic of digital terrorism as an innovative threat to cyber security by defining its concept and impact on international peace and security.

Keywords: digital terrorism, cyberspace, international peace and security, digital attacks, digital attacks.

01

Introduction

The world has witnessed a remarkable transformation driven by the rapid expansion of information technology. Digital networks and advanced technological tools have become indispensable in the lives of individuals and organizations alike.

Moreover, they now serve as a fundamental benchmark for assessing a nation's scientific and technological progress.

Consequently, the concept of national infrastructure has shifted toward a virtual, digital framework that relies on digital networks for storing and managing essential state data. Initially, the use of digital technologies was confined to the public sector, particularly state institutions.

However, as these technologies became more widespread, new threats emerged, posing significant risks to their integrity and security.

This growing vulnerability has made it imperative to develop protective measures against potential cyber threats, giving rise to the concept of cybersecurity.

The digital transformation of modern international society has also introduced new challenges, particularly in the form of cybercrimes.

These crimes involve the unlawful exploitation of digital tools through hacking, electronic infiltration, and cyberattacks aimed at disrupting a country’s digital infrastructure or gaining access to classified government data.

Such attacks often target intelligence agencies, causing substantial financial, material, and even human losses. Given their borderless nature and high-speed execution, cybercrimes have been recognized as international offenses, prompting nations and global organizations to intensify efforts to combat them.

In response to these growing threats, the international community has taken steps to establish legal and institutional frameworks, along with preventive measures, to safeguard nations and individuals.

Cybersecurity, in this context, refers to a set of legal, technical, and operational mechanisms designed to ensure the protection of digital systems and sensitive data, whether belonging to states, international organizations, or private entities.

Cybersecurity is now a cornerstone of global stability, safeguarding both national infrastructures and international security.

Despite the legal and institutional efforts made to counter cybercrimes, these measures remain insufficient in addressing the advanced intelligence and sophisticated tactics employed by cybercriminals.

Their professionalism and ever-evolving techniques continue to pose a significant challenge to global cybersecurity efforts.

02

One of the most pressing threats to national electronic security is the rise of digital attacks carried out by terrorist groups, these attacks represent an evolution and extension of traditional extremist tactics, adapting to technological advancements.

Historically, terrorism has been a significant threat to international peace and security, primarily relying on conventional armed force and military weapons. However, with the digital revolution, terrorist groups have shifted their strategies, embracing cyber warfare as a more potent and elusive form of attack.

Unlike traditional terrorism, cyberterrorism is characterized by its technical complexity and difficulty in attribution, making it a formidable challenge for global security agencies.

Given this shift, combating cyberterrorism has become a top priority for the international community. Recognizing its potential to destabilize nations, governments and global organizations have increasingly turned to cybersecurity as a primary defence mechanism.

Cybersecurity encompasses a range of technical and legal measures aimed at countering cyber threats and safeguarding digital infrastructures, this leads us to a critical question: How effective is cybersecurity as a preventive and deterrent measure against the rising dangers of cyberterrorism?

Research Axes:

to explore this issue, our study is structured around the following key areas:

A Conceptual Introduction to Cybersecurity and Cyberterrorism.

The Impact of Terrorist Groups on International Peace and Security.

Axis One:

A Conceptual Introduction to Cybersecurity and Cyberterrorism

The Concept of Cybersecurity: also referred to as information security, is a specialized system designed to protect individuals, organizations, and digital infrastructures from cyber threats, including illegal hacking, digital espionage, and electronic sabotage.

The need for cybersecurity arose in response to the increasing prevalence of digital virus attacks, which compromise systems by gaining unauthorized access to sensitive data.

These cyber threats often serve purposes such as theft, blackmail, or large-scale digital sabotage.

An essential function of cybersecurity is identifying and addressing vulnerabilities within digital systems, preventing potential security breaches before they occur.

By implementing advanced protective measures, cybersecurity helps mitigate the risks posed by cyberterrorism and other digital crimes.

Definition of Cybersecurity:

In its broadest sense, is defined as a state of inner peace and the absence of fear.

While traditionally associated with physical protection, the modern concept of security has expanded to include digital security, reflecting the increasing reliance on digital infrastructures in all aspects of life.

Cyber Terrorism and the Exceptions to the Prohibition of Force in International Law

International Peace and Security Measures (Chapter VII of the UN Charter) The second exception to the principle of prohibiting the use of force in international relations is the enforcement of international peace and security measures as stipulated in Chapter VII of the United Nations.

Article 39 of the UN Charter allows the UN Security Council to determine whether an act constitutes a threat to peace, breach of peace, or an act of aggression.

If a cyber-attack is classified as such, the Security Council may take action, including: Sanctions Cyber countermeasures Military interventions in extreme cases

International Humanitarian Law and Cyber Warfare the First Additional Protocol to the Four Geneva Conventions of 1949 established a legal framework for evaluating new combat methods, requiring that each new weapon undergo legal review to ensure its compliance with international law (Article 36). Application to Cyber Warfare Cyber weapons and attacks must be assessed for their legality under

international humanitarian law (IHL).

03

The Tallinn Manual, published by NATO's International Committee, argues that IHL applies to cyber warfare because it can constitute an international armed conflict.

The Martens Clause and Cyber Conflict the Martens Clause (found in the Hague Conventions of 1899 and 1907 and later treaties) provides that, in the absence of specific

treaty law, conflicts should still be governed by customary international law and the principles of humanity and conscience.

The International Court of Justice (ICJ) confirmed in its 1996 Advisory Opinion on nuclear weapons that new types of warfare must comply with international humanitarian principles.

Protection of Civilians in Cyber Warfare Distinction Between Civilian and Military Targets Article 50(1) of the First Additional Protocol (1977) states that civilians must not be the target of cyber-terrorist attacks, however, cyber warfare complicates this distinction, as cyber-attacks often affect civilian and military systems simultaneously may spread beyond their intended targets, causing collateral damage.

Prohibition of Indiscriminate Attacks Article 51 of the First Additional Protocol (1977) prohibits attacks that cause excessive civilian harm.

Cyber-attacks that disrupt hospitals, financial institutions, or public infrastructure could violate this principle.

The Principle of Humanity, this principle, a cornerstone of IHL, ensures that basic human rights are protected even during war.

Cyber terrorism that disrupts essential services (e.g., power grids, water supplies, healthcare systems) could be classified as a violation of humanitarian law.

Security measures are commonly linked to the protection of citizens from potential threats to their safety and property.

This protection is ensured through the establishment of laws and regulations. Additionally, it involves responsible authorities that create and enforce these legal and security frameworks.

National security measures include a broad range of protective actions, from proactive strategies to safeguard the state against threats to strict border control regulations, protection of classified information, and the formulation of a comprehensive national security strategy.

These measures also involve military forces, alliances, and initiatives aimed at maintaining economic and social stability.

Cybersecurity, on the other hand, specifically pertains to protecting information systems, data, and services from unauthorized access, damage, misuse, or human errors caused by system operators who fail to adhere to security protocols.

Cybersecurity is also considered a national security measure designed to prevent cyberattacks from hackers and implement effective countermeasures.

Legal scholar Edward Abelson defines cybersecurity as a set of technical methods to reduce risks associated with attacks targeting software, computers, and networks, these methods include tools to prevent hacking attempts, detect and block malware, and provide secure communication channels. The International Telecommunication Union (ITU) describes cybersecurity as a combination of tools, policies, security principles, safeguards, risk management strategies, procedures, training, best practices, and assurance mechanisms.

These elements are integrated within networked environments to protect organizational assets, such assets encompass network computing devices, personnel, infrastructure, applications, services, communication systems, and information that is either transmitted or stored within a digital environment. The core aim of cybersecurity is to establish, maintain, and safeguard institutions and users from risks associated with digital networks.

Its fundamental objectives include ensuring availability, integrity—which may involve authentication and non-repudiation—and confidentiality.

04

Modern society is becoming increasingly reliant on information and communication technologies linked to the World Wide Web. However, this widespread dependence introduces various emerging and potential risks that pose significant threats to network and information security.

Members of the information society face daily challenges due to the misuse of digital networks for criminal activities.

Protecting critical national information infrastructure, particularly sensitive personal data, is a fundamental aspect of cybersecurity and plays a crucial role in both national and international security policies.

3.Components of Cybersecurity:

Cybersecurity is built on three essential components:

a. Technical Tools and Infrastructure: This includes the core technological foundations of information systems, such as the internet, communication networks, computer systems, and embedded processors. Maintaining cybersecurity requires implementing a combination of technical, physical, and legal measures to safeguard these systems effectively.

b. Human Element: This category involves programmers, system users, and specialists in fields like information technology, artificial intelligence, and electronics, it also includes senior engineers and technicians whose expertise is vital for the effective deployment and management of cybersecurity strategies.

c. Specialized Capabilities and Resources: Cybersecurity also depends on specialized expertise in various technological domains, these skills are essential for maintaining and strengthening digital security systems.

3. Cybersecurity Goals

The primary objective of cybersecurity is to prevent unauthorized access, this begins with ensuring data integrity during storage, processing, and transmission while maintaining uninterrupted service for legitimate users.

Users also benefit from improved information protection, ensuring continuous functionality and security.

In the same context, cybersecurity focuses on maintaining a secure flow of information while ensuring its authorized and lawful transfer.

Additionally, it aims to swiftly recover any leaked data in the event of a cybersecurity breach.

Cybersecurity Concepts and Actors

Cybersecurity encompasses several key concepts. Cyberattacks refer to actions that compromise the functionality or capabilities of a computer network, often for national or political motives, by exploiting specific system vulnerabilities, in contrast, cybercrime involves a range of illegal activities and behaviours carried out using electronic devices, digital networks, or technological systems.

Such crimes demand advanced expertise in computing and cybersecurity, often targeting sensitive state secrets or critical infrastructure.

Regarding the key actors in cybersecurity, they include:

States: A state is a legal and internationally recognized entity, defined by three fundamental components: territory, population, and political authority, along with a fourth element—international recognition.

In the field of cybersecurity, states with advanced technological resources capable of executing cyberattacks are primary players, given their extensive digital reach, states often hold a dominant role in the cyber landscape, surpassing many other actors in influence.

Non-state actors: This category covers various entities, starting with multinational corporations, some of which hold economic power exceeding that of certain nations, granting them significant influence on the global stage.

It also includes criminal organizations engaged in hacking, data breaches, financial fraud, and cyber theft. Additionally, terrorist groups have increasingly relied on digital platforms for recruitment, fundraising, propaganda, and strategic planning, another noteworthy non-

state actor is the individual hacker, who has gained prominence—often in controversial ways—in the cybersecurity domain.

05

Axis two

The Concept of Cyberterrorism is essentially an extension of traditional terrorism, a term that scholars in international law have struggled to define consistently.

The concept of terrorism has long been a subject of debate among experts, as it remains broad and open to various interpretations; Additionally, international efforts have sought to define terrorism as a phenomenon. Generally, terrorism involves the organized execution of actions such as assassination, sabotage, murder, hostage-taking, planting explosives, and hijacking, alongside other unlawful acts.

Legally, Article 1 of the 1937 Geneva Convention for the Suppression and Punishment of terrorism classifies terrorism as criminal acts directed against a state with the intent of spreading fear and terror within specific communities, Similarly, the United Nations Security Council, acting as an international executive body, sought to define terrorism in Resolution 1566.

It identified terrorism as any criminal act targeting civilians with the intent to kill, harm, or injure them, or attempting to pressure or coerce a government or international organization into favouring a terrorist group.

Definition of Cyberterrorism differs from other forms of terrorism due to its modern approach, which relies on the use of digital resources and electronic tools to disrupt systems and threaten the informational infrastructure of states.

It encompasses three key elements: cyberspace, terrorism, and the virtual domain, which is based on the symbolic and artificial representation of information.

Some researchers describe cyberterrorism as a convergence of criminal power and cyberspace, creating risks to peace and security in pursuit of criminal goals such as the intimidation of individuals and governments.

Characteristics of Cyberterrorism is distinguished by several unique features, the most notable being its lack of reliance on physical force or direct violence to execute its attacks, instead, it operates through computers connected to the internet, utilizing specialized digital programs, with the continuous expansion of digital networks worldwide, cyberterrorism transcends national borders, making it a global and transnational threat that is not confined to a single state's territory.

Due to the complexity of the internet and digital software, cyberterrorist activities are particularly challenging to detect, largely because of the general lack of cybersecurity expertise among users, including security and judicial personnel.

One of the most significant challenges in combating cyberterrorism is the difficulty in gathering evidence. The rapid erasure and destruction of digital traces make investigations complex.

Additionally, cyberterrorism is recognized as an organized crime that typically involves the collaboration of multiple individuals, those engaged in such activities are often members of terrorist groups with advanced technical expertise in information technology and cyber operations

Objectives of Cyberterrorism

Cyberterrorism serves a variety of illicit purposes, primarily aimed at instilling fear and chaos within both domestic and international communities. By doing so, it undermines peace and security on a global scale.

Among its main objectives are the disruption and destruction of national information infrastructures, the targeting of digital and technological resources, the destabilization of economies, and the sabotage of public and private institutions.

06

Section Two:

The Impact of Terrorist Groups on International Peace and Security

Digital terrorism has emerged as a significant concern for the international community due to its reliance on so-called “digital violence” to achieve political, economic, ideological, and military objectives, among others. This poses a threat to global stability, compelling us to examine the impact of terrorist groups on international peace and security.

In this section, we will first explore how cyberterrorism endangers global peace and security, then delve into the legal framework surrounding cyberterrorist attacks under international law, and finally, review international efforts to combat digital terrorism.

First:

Manifestations of Cyberterrorism’s Threat to International Peace and Security

It is essential to recognize that the primary driver behind the spread of cyberterrorism is, above all, the weaknesses in states' cybersecurity policies and the fragility of infrastructure protection programs within each country.

These vulnerabilities increasingly affect national security and pose a serious threat to both international peace and stability.

This phenomenon has intensified significantly, particularly after 2011, as various conflicts and wars—such as the Arab Spring uprisings and the Russia-Ukraine conflict—

have exposed critical weaknesses, similar to those seen in the breaches of the Russian Research Agency.

The threat of cyberterrorism to peace and security lies in its ability to exploit global connectivity between the internet and international satellite systems, linking all nations. Additionally, advancements in technical skills have led to the development of new forms of weaponry that facilitate espionage, requiring only technical expertise to carry out cyber-attacks.

These invisible weapons have proven highly effectiveness in dismantling the digital systems of states, potentially leading to paralysis in government operations.

07

Second:

The Legal Nature of Digital Terrorist Attacks in International Law

1.Applying the Rules of Public International Law to Cyberattacks One of the fundamental principles of international legal relations is the prohibition of the use of force, as stated in Article 2, Paragraph 4 of the United Nations Charter.

Some legal scholars argue that cyberattacks fall under this principle, as they can threaten state stability and impact civilian lives. However, this interpretation is debated, with some experts, such as Marco Rossini, asserting that the term "force" in the Charter specifically refers to military actions rather than cyber operations.

Despite the general prohibition of force, international law acknowledges certain exceptions. The most notable is the right to self-defence, outlined in Article 51 of the UN Charter.

However, the International Court of Justice has historically applied a strict interpretation of this right, for example, in the 1986 Nicaragua case, the Court ruled that self-defence must meet specific criteria, including proportionality and necessity. Therefore, cyberterrorism—when involving cyberattacks aimed at compromising a state's sovereignty and security—could, in certain circumstances, justify the use of self-defence as a means to mitigate its threats.

The second exception to the principle of non-use of force in international relations is the implementation of measures aimed at preserving international peace and security.

According to Chapter VII of the United Nations Charter, the Security Council has the authority to take such measures in response to any act of international aggression, in accordance with Article 39 of the Charter.

2.Applying International Humanitarian Law to Cyberattacks

Article 36 of the Additional Protocol I to the 1949 Geneva Conventions establishes a general framework for evaluating the means used in combat operations, including emerging methods of warfare, this article requires an assessment of the legality of any newly developed or acquired weapon, reaffirming that the principles of International Humanitarian Law (IHL) remain applicable to all weapons as long as armed conflicts persist. In the absence of specific regulations, these general legal principles govern warfare during conflicts.

In this context, NATO's Cooperative Cyber Defence Centre of Excellence introduced the "Tallinn Manual," which asserts that international humanitarian law applies to cyber warfare, as it constitutes an extension of armed conflict. Furthermore, the Martens Clause—embedded in the preambles of both the 1899 and 1907 Hague Conventions and later reaffirmed in Additional Protocol I (1977) and Additional Protocol II—upholds the protection of combatants under customary international law and principles of international conscience, even in cases where no specific treaty exists.

The International Court of Justice reinforced this principle in its 1996 advisory opinion on the legality of the threat or use of nuclear weapons.

Additionally, the distinction between civilian and military targets, as outlined in Article 50(1) of Additional Protocol I (1977), establishes that civilians must not be targeted in acts of digital terrorism, However, mitigating the effects of cyberattacks remains a significant challenge, as attackers often operate remotely, far from their intended targets.

08

Conclusion

Cyberspace has evolved into a vast and intricate domain that transcends physical boundaries, profoundly influencing global economic, political, and cultural landscapes.

Its impact extends even into military affairs, where nations are rapidly integrating advanced technologies into their weapon systems.

However, terrorist groups have also embraced these digital innovations, giving rise to cyberterrorism—an emerging threat that disrupts cybersecurity by exploiting the virtual realm to achieve criminal objectives.

Cyberterrorism has become one of the most significant threats to international peace and security, surpassing traditional terrorism in its reach.

Due to its heavy reliance on technology, its consequences are not confined to the borders of a single nation but rather have far-reaching global implications.

As a form of warfare, cyberterrorism falls under the principles of international humanitarian law, as its actions have the potential to provoke declarations of war.

This legal framework is particularly reinforced by the Tallinn Principles, which were established through Additional Protocol I of the 1977 Geneva Conventions.

List of Sources and References Used:

First: Sources and References in Arabic

Sources:

United Nations Charter.

Geneva Convention on "Suppression and Punishment of Terrorism," issued in 1937.

Additional Protocol I to the Geneva Conventions, adopted on August 12, 1949, concerning the protection of victims of international armed conflicts, adopted and opened for signature, ratification, and accession by the Diplomatic Conference to reaffirm and develop international humanitarian law applicable to armed conflicts, dated June 8, 1977, effective as of December 7, 1978, under Article 95.

United Nations Security Council Resolution No. 1566, Session No. 5053, issued on October 8, 2004.

Resolution 181 of the International Telecommunication Union, Recommendation x.1205, Guadalajara, 2010.

References:

Books:

Ahmed Hussein, Cybersecurity Challenges and Their Impact on International Security, 2nd edition, Dar Al-Jil, 2019.

Hussein Al-Azawi, The Position of International Law on Terrorism and Armed Resistance, Dar Al-Hamed for Publishing and Distribution, DSN.

Adel Abdel Sadiq, Cyber Weapons in Light of International Humanitarian Law, Library of Future Studies Unit, Alexandria, Egypt,2015.

Adel Abdel Sadiq, Electronic Terrorism: A New Pattern of Power in International Relations, Center for Political and Strategic Studies, Egypt, 2009, p. 115.

Fares Mohammad Al- ‘Amarat, Cybersecurity: Concept and Challenges of the Era, Dar Al-Khaleej for Publishing and Distribution, D.P.N., 2020.

Farah Yahya Zaatarah, Cyber Threats to U.S. National Security, Arab Publishing and Distribution, D.S., P.N. Mohamed Abdullah, Cybersecurity and Protection of the International System, 1st edition, Dar Al-Fikr Al-Arabi, 2020.

Mohamed Kamal, When the Terrorist Uses the Keyboard Instead of the Bomb, Dar Kleem for Publishing and Distribution, Egypt, 2022.

Mustafa Mahmoud Manjoud, The Political Dimensions of the Concept of Security in Islam, International Institute for Islamic Thought, Egypt, 1996. Najdat Sabri Thakari, The Legal Framework for National Security: An Analytical Study, Dar Dijla, Amman, 2011.

09

Articles:

Ahmed Al-Fatlawi, Cyber Attacks: Their Concept and the Emerging International Responsibility in Light of Contemporary International Regulation, Journal of Local Investigator for Legal and Political Sciences, Issue 4, Volume 8, 2016.

Inas Mamdouh Mohamed Mohamed Suleiman, The Role of Cybersecurity in Facing Electronic Terrorism, Journal of Legal and Economic Sciences, Issue 01, Volume 64, 2022.

Hamidi Hayah Tayeb Naseemah, Introduction to Cybersecurity Concepts, Journal of Digital Communication Studies, Volume 02, Issue 02, 2022.

Sharifa Klah, Cybersecurity and Challenges of Cyber Espionage and Breaches by States in Cyber Space, Journal of Rights and Human Sciences, Volume 15, Issue 01, 2022.

Ali Adnan Al-Fil, Electronic Terrorism, Gulf University Journal, Law Department, Issue 2, University of Mosul, Iraq, 2010.

Mohamed Hassan Said Draji, Cyber Attacks According to the Provisions of International Humanitarian Law, Journal of Sharia and Law Studies, Volume 51, Issue 1, 2024.

Hani Mohamed Khalil Al-Azazi, The International Legal System to Combat Cybersecurity Risks, Contemporary Egypt Journal, Issue 549, 2023.

Conferences:

1. Aysar Mohamed Atiyah, The Role of Modern Mechanisms in Reducing Emerging Crimes - Electronic Terrorism and Its Countermeasures, Article presented during the conference on Emerging Crimes in the Context of Regional and International Changes and Transformations, held from 2-4 September 2014, Faculty of Strategic Sciences, Amman, Jordan, 2014.

4- Websites:

Ayman Hussein, Electronic Terrorism: The Most Dangerous Battles in Space Wars, Article available at the following link: .

RafdAyadah Al-Hashimi, Electronic Terrorism, eBook available at the following link: .

Second: Sources and References in Foreign Languages:

Herbert Lin, Cyber Conflict and International Humanitarian Law, International Review of the Red Cross, 2012, Vol. 94, No. 886, p. 515.

Doswald-Beck, International Humanitarian Law and the Advisory Opinion of the International Court of Justice on the Threat or Use of Nuclear Weapons, ICRC, Vol. 316, 1997.

10