International Perspective on Securing Cyberspace Against Terrorist Acts

Maya Hasan Khater, Al Yamammah University, Saudi Arabia*

https://orcid.org/0000-0002-5892-9176

ABSTRACT

This research reviews the legal framework for protecting the security of cyberspace from terrorist acts, using the following approaches: the legal approach, the descriptive approach, and the analytical approach. This is achieved by gathering knowledge and data on the protection of cybersecurity and analyzing the different tools and methods that terrorist organizations use to implement their cybercrimes. The goal is to find ways to overcome the various challenges that terrorists pose to regional (Arab-wide) and international cybersecurity systems to find mechanisms and solutions to deal with this phenomenon effectively and to reduce its increasing risks to people and the security, stability, and economies of nations. The most significant conclusion that was reached is the need to continue international efforts to strengthen the fight against cyberterrorism and to establish a binding legal treaty in this regard so as to prevent further harm to the safety of the international community.

KEYWORDS

Combating International Terrorism, Cyber Terrorist Attacks, Cybersecurity, Cyberterrorism, Internet Studies, Sociotechnical Studies, Technology in Society, Terrorist Crimes

INTRODUCTION

Cybersecurity is an important issue due to the expanded use of the internet and mobile devices in commerce, government, and everyday life. Cybersecurity is the defense of computer systems against threats like theft, hardware damage, corruption of software and data, and interruption or rerouting of services (Wang & Wang, 2021).

Cyberspace is a new arena for disruptive terrorist attacks; therefore, its protection from cyberterrorism is a global concern. Terrorists can exploit advanced information technologies, sociotechnical systems, and communication systems to carry out criminal activities against vital infrastructures, spread propaganda, and benefit from recruitment and funding (Woodhead, 2012).

The evolution of international terrorist crimes is alarming. Terrorists use digital technologies (i.e., internet, mobile phones, and computer networks) to commit criminal acts and spread fear among individuals, institutions, and governments. The urgency to study the protection of cybersecurity

DOI: 10.4018/IJSKD.318706 *Corresponding Author

This article published as an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.
through a counterterrorism lens stems from rapid developments in technology, society, politics, and economics that impact our daily lives.

The number of websites run by terrorist organizations has increased significantly over the past few years. Hundreds of websites serve terrorists and their supporters, allowing these organizations to have a presence in cyberspace (Weimann, 2006). Digital platforms are low cost with a high impact, allowing users ease in committing cybercrimes while maintaining anonymity. Information technologies make it simple to create or hack websites, spread spyware and destructive programs, transmit or publish information (i.e., data, statements, and films), and promote ideas and advocate for recruitment and mobilization.

This study addresses the protection of cyberspace from terrorist acts, including coordination and communication, spying on and destroying websites, media promotion, and propaganda wars for funding and recruitment. The current research discusses regional efforts to counteract cyberterrorism and international community efforts like the role of the United Nations (UN) in cybersecurity. The research offers recommendations and suggestions to achieve stronger security in cyberspace.

FOCUS OF THE ARTICLE

Today, cybersecurity is a prioritized research topic. The objective of this article is to create public awareness surrounding electronic crimes and acts of cyberterrorism in our daily lives. It is evident that cyberattacks are increasing across the globe. In addition, they continue to involve more advanced technologies like malware, encrypted messaging services, spyware, and information theft. These methods demonstrate the urgent need to develop a framework to coordinate the efforts of international and regional institutions in dealing with cyberterrorism.

LITERATURE REVIEW

Cyberspace is a pervasive network that connects every field of contemporary culture. Cyberattacks have become prevalent. Securing cyberspace is, therefore, a major concern of governments around the world. Researchers have been developing standards and innovative methods to strengthen cybersecurity policy, enhancing the security of critical infrastructures and implementing national defensive countermeasures (Vaseashta et al., 2014). Effective frameworks are required to facilitate the use of data analytics to anticipate attacks, identify optimal countermeasures to respond to attacks, and optimize the allocation of resources after an attack (Shahin et al., 2020).

Cyberattacks are classified based on a range of actions. Some attacks involve data and information theft. Others shut down entire systems. Attacks may be motivated by political unrest or social or economic problems. Cyberattacks can even involve espionage that promotes political and financial agendas (Karlidag & Bulut, 2020).

Many authors have identified cyberterrorism and cyberattacks as armed attacks that pose a threat to international security. These authors have attempted to understand the applicability of the rules and provisions of the UN charter to cyberattacks, as well as how these attacks violate domestic and international law. They suggest appropriate responses that countries can use to reduce or eliminate the risks associated with cyberterrorism and cyberattacks. One important strategy is to finalize a multilateral treaty to maintain international peace and security by preventing the use of cyberattacks and removing loopholes that can be exploited by terrorists (Mahnoor & Noor, 2022).

Some suggest that terrorism is the most significant challenge faced by humanity. Due to the lack of comprehensive data, it is difficult to predict cyberterrorist operations or identify conspirators. Therefore, we must analyze data related to terrorist attacks to prepare algorithms that anticipate and predict attacks (Alfatih et al., 2019).

Cybersecurity approaches and strategies must focus on promoting transparency and achieving international cooperation (Kovács, 2018). There is also a need for a collaborative security strategy
based on the sharing of information to develop preventative measures and protect cyberspace from cyberattacks (Feltus, 2019).

Authors have argued that governments should play a role in protecting sensitive information from cyberattacks. This can be achieved by ensuring the secure storage of data, including the creation of mechanisms to retrieve encrypted data while maintaining query privacy (Mohammed et al., 2021). Protective mechanisms should not only focus on detecting cyberattacks. They must define their pathways, providing immediate protection for network devices when attacks are detected (Hosny et al., 2020). Authors are also interested in governance, security, and organizational tactics that advance cybersecurity (Mahajan et al., 2018).

The current study’s findings are consistent with previous findings in the literature. The literature has, however, been limited to general discussions on defending cybersecurity against cyberattacks. The current study builds on this foundation by examining the legal aspects of cybersecurity associated with cyberterrorism at regional and global levels. It identifies mechanisms and solutions, providing a set of recommendations and initiatives to improve cybersecurity and address cyberterrorism.

Many efforts have been made to combat cyberterrorism at regional and international levels. There are also many achievements in the legal and institutional sectors. However, there is still a pressing need for measures that confront risks posed by cyberterrorism. Steps should be taken to address these risks to prevent cyberspace from becoming a dominant arena for interstate wars and conflicts. Priority should be given to the goal of improving early detection systems to anticipate and prevent attacks.

**METHODOLOGY**

The descriptive analytical method was used to investigate the legal dimensions of cybersecurity associated with cyberterrorism. This includes the identification of protective mechanisms that can be utilized in security. Additionally, the structural method was used to describe cyberterrorism as a set of criminal acts, the mechanisms that are exploited when using cyberspace for terrorist purposes (i.e., coordination and communication, spying on and destroying websites, media promotion, and propaganda war for funding and recruitment), and regional and international community efforts and initiatives to combat cyberterrorism.

The ideas in this article are supported by the analysis of regional and international treaties, international resolutions and documents, and official reports by international institutions. This forms the foundation for a set of recommendations aimed at improving cybersecurity practices in response to cyberterrorism.

The descriptive analytical method is employed in this research because of its flexibility and comprehensiveness. It enables the accurate study of phenomena through the analysis of causes and identification of optimal solutions. To achieve its objectives, the study includes an examination of the significant literature on cybersecurity and terrorism. This systematic review of the literature is used to make recommendations based on available data (Aridi, 2022; Burrell, 2021; Iyamu, 2020).

The results of this research may be interesting to academics from a theoretical perspective. It could also be useful to policymakers and other actors.

**Cyberterrorism**

Artificial intelligence (AI) has impacted many fields of security and intelligence. The use of AI and big data in the areas of intelligence and counterterrorism has sparked discussions between those who support its continued use and those who oppose its expansion. There is a difficult balance between efficacy in the war on terrorism when counterterrorism uses AI and big data technology. The liberal democratic principles of society become even more important.

Cyberterrorism mirrors cybercrimes, terrorism, espionage, fraud, and information piracy. In fact, they are all criminal activities that constitute a behavior or criminal outcome. It is difficult to formulate a clear legal definition of this relatively new type of crime (Anderson, 2010). The issue
of developing a specific and accepted definition of international terrorism remains an intractable problem. However, the reason for not agreeing on a specific definition of terrorism is not due to the ambiguity of the term or a lack of vocabulary. The challenge relates to the desire to disagree based on divergent views and political wills that underscore differing ideologies and interests. While some see it as terrorism, others see it as a legitimate act or fight for freedom from colonial oppression (Meisels, 2009). As noted by Ganor (2002), “a freedom fighter for one person is a terrorist for another” (p. X).

There have been many regional and international attempts to define terrorism despite the absence of a universally accepted definition (The United Nations Office on Drugs and Crime, 2012). Arab efforts in the field of international counterterrorism culminated in the adoption of a definition of terrorism, defining it as any violent action or threat of violent action, regardless of its justifications or objectives, that is carried out in the course of a criminal enterprise designed to terrorize, intimidate, or harm people, endanger their safety, security, or liberties, damage the environment, harm private or public property, occupy or seize such property, or put national resources at risk (The Arab Convention for the Suppression of Terrorism, 1998).

Cyberterrorism occurs at the meeting point between terrorism and cyberspace. This is the exploitation of computers, networks, and information in carrying out terrorist attacks and threats (Weimann, 2004). The term “cyberterrorism” refers to acts of terrorism committed using digital technologies with political, ideological, or religious motives to intimidate countries, groups, or individuals, cause severe damage (death or financial harm), and influence government decisions or public opinion (Denning, 2002). When terrorists use technology for economic rather than political motives, the crime is classified as an electronic crime rather than cyberterrorism (Gable, 2010).

Cyberterrorism includes all uses of technology in activities that serve terrorist purposes. This includes incitement, such as inciting hatred and disputes, spreading extremist ideas, coordination and communication, financing and recruitment, and the implementation of terrorist acts. Cyberterrorism involves the use of violence, fear, and terror by an individual, group, or state that is politically motivated to disturb order, destabilize security and tranquility, and disrupt electronic control and monitoring systems that endanger the safety and security of society. It may lead to the disruption of governmental facilities, agencies, and private institutions. It may also harm basic freedoms and violate human dignity. For this reason, cyberterrorism falls within the category of cybercrimes that aim to control information systems, sow fear, chaos, and distrust of technology systems, steal or disseminate information, finance terrorist operations, and facilitate terrorist recruitment (Gross et al., 2016).

Terrorists are drawn to cyberterrorism for several reasons. First, it is less expensive (a laptop and Internet connection) than more conventional terrorist tactics. Second, cyberterrorism is anonymous, making it difficult for security organizations and police forces to identify the terrorists. Third, cyberterrorism requires less physical preparation, psychological commitment, and risk of death. It is, therefore, easier to recruit and retain supporters. Finally, compared to traditional terrorist tactics, cyberterrorism can harm more individuals, resulting in extensive media coverage and visibility (Weimann, 2004).

**Mechanisms of Using Cyberspace for Terrorist Purposes**

Cyberterrorism is characterized by terrorist groups who exploit technological progress (information and communications technology) to plan and organize their acts. There is a potential of severe economic, social, and political damage that may undermine the authority of the state, threaten national security, and harm a national economy or foreign investments.

**Coordination and Communication**

Terrorist groups use e-mail, social networks, forums, and other modern means of communication as an inexpensive, broad medium to communicate and exchange information or proposals among members. The groups can plan their operations online, reducing the risks that arise from direct meetings. They can also avoid the use of traditional (traceable) means of communication. Terrorists hack personal e-mail, track correspondence, and gain access to personal and confidential data to benefit the planning
of terrorist operations. Terrorists also use technologies to spread their ideas, promote their work, and gain sympathy. In this context, terrorists hack e-mail to track correspondence and view confidential data to help in their planning of terrorist operations (Denning, 1999).

For example, Tom Metzger, an infamous American extremist, founded the White Aryan Resistance Group to preserve the purity of the White race. Metzger is considered one of the first to employ electronic means to communicate and share ideas. For instance, he used e-mail to communicate with his followers and distribute his speeches (Michael, 2016).

Terrorist sites aim to provide theoretical or ideological education. They also supply audio/video training clips to teach members how to hide and erase evidence from police, manufacture explosive belts and bombs, disrupt or destroy counterterrorism websites, spread computer viruses, and plan or coordinate terrorist acts. They are, thereby, turning electronic platforms into virtual training camps (The United Nations Counter-Terrorism Implementation Task Force, 2011).

Spying on and Destroying Websites

Technology can be used as a means of coordinating and communicating with terrorist organizations. In addition, it can spy on and penetrate websites or computers. Computer hackers who work for terrorist organizations use programs to watch networks and electronic systems, attacking vital information infrastructures (i.e., e-mail, subscriber lists, credit card information, and passwords) of governments and private institutions (Valeri & Knights, 2000).

Cyberterrorists use electronic viruses and spyware to destroy and distort data, information, and computer programs. They want to obtain information related to vital places and installations that terrorist operations can target or destroy. They also aim to disable computers and programs. The data on the target computer is then scattered and transmitted to the hacker’s device. For example, terrorist groups may attack the control systems of transportation systems, which leads to ground and air traffic disruptions or collisions between planes and trains. Terrorists also target installations (i.e., electricity, gas, and oil) to weaken confidence in the national economy and official institutions. They may also disrupt financial operations by banks or penetrate safety systems in factories and hospitals (The United Nations Counter-Terrorism Implementation Task Force, 2011).

Russia’s cyberattacks on Estonian infrastructures in 2007 is an example of a targeted attack on a basic infrastructure. This attack included the defacing of websites and e-mails by the Estonian government and political institutions. Terrorists also used the attack to disrupt internet services (Schmidt, 2013). The drones that belonged to the Houthi rebels in Yemen are another example of a cyberattack. These drones attacked oil refineries in the Abqaiq and Khurais fields in Saudi Arabia on September 14, 2019, causing severe damage to Saudi oil facilities. This attack was complemented by additional acts on civilians and Saudi installations (Defterios & Cavaliere, 2019). Russian cyberattacks on Estonia can be defined as acts of state terrorism. The Houthis’ repeated exploitation of Saudi cyberspace was committed by a terrorist organization. Nevertheless, both acts should be rejected for flouting international laws and norms. In addition, their consequences undermined international peace and security.

Media Promotion

Many websites affiliated with terrorist organizations seek to publish propaganda (i.e., statements, books, videos, and pamphlets) that disseminates extremist ideas adopted by the terrorist group. These websites spread false or misleading news. They target security services and public opinion. The opinions cause divisions (religious and ethnic) and spread defamatory information about individuals and institutions. This, in turn, can incite terrorist acts against groups. Terrorists use technology to spread a culture of violence by encouraging acts of terrorism and excessive use of violence through horrific text, images, recordings, and electronic games. At the same time, it spreads a state of terror and fear (The United Nations Office on Drugs and Crime, 2012).

With the increase in the use of informatics, the internet has become an important means by which terrorist organizations document their operations and glorify perpetrators. They publish films that document
the planning and execution of terrorist acts. They also distribute statements from organizers. Perhaps the most prominent examples are films published by websites affiliated with the Islamic State in Iraq and Syria (ISIS). For example, these films showed Jordanian pilot Moaz al-Kasasbeh being burned alive (Syrian Network for Human Rights, 2015). ISIS militants also published a video depicting the slaughter of Egyptian Copts taken hostage (Guerin, 2015). In 2019, a terrorist who gunned down dozens of worshipers in two mosques in New Zealand streamed his crimes live on Facebook (Gelineau & Gambrell, 2019).

These are some of the many instances in which terrorists have used the Internet, with the help of advanced imaging technologies and audio-visual effects, to influence their audience. They use emotion to gain affection, support, or membership. They also intimidate their audience, weakening their morale and discouraging them through threats and fear.

There is a close link between the activities of extremist terrorist organizations and the use of social media platforms. Terrorists exploit social media for many reasons, including the promotion of extremist beliefs through online media, propaganda, narratives, operational information, and recruitment efforts via cyberspace. Therefore, addressing cyberterrorism must begin with cracking down on both the producers of online terrorist propaganda and consumers.

Propaganda War for the Purposes of Funding and Recruitment

Some websites affiliated with terrorist groups promote the ideology and principles adopted by these groups. They aim to increase the number of supporters and strengthen the positions of their followers/sympathizers (Weimann, 2006). Websites and other modern technologies can facilitate financial and logistical support for terrorist activities. This may be achieved by force, such as seizing the accounts of bank customers. Activities also include money laundering, drugs, weapons, human trafficking, and fraudulent schemes like humanitarian and volunteer organizations that funnel donations to bank accounts held by terrorist organizations. Additionally, technology can be used as a tool for recruiting and mobilizing members for financing, communicating, and supporting terrorism and extremism along with the dissemination of false information and “fake news” (The United Nations Office on Drugs and Crime, 2012).

Efforts of the International Community to Counteract Cyberterrorism

The international community has attached great importance to countering cyberterrorism as countries become more aware of the ways in which terrorists use digital technology to achieve their goals. This section discusses steps that have been taken to combat these crimes and counteract threats to the security and safety of society.

Regional Efforts to Counteract Cyberterrorism

Arab countries have created several agreements related to combating terrorism in an attempt to uncover the causes of terrorism and eradicate resources of terrorist organizations. The most important are the Treaty of the Organization of the Islamic Conference to Combat International Terrorism (1999), the Arab Convention to Combat Terrorism (1998), and the Cooperation Council Convention for the Arab States of the Gulf to Combat Terrorism (2004).

Arab countries have also ratified several documents related to preventing cybercrime, including cyberterrorism, and preserving their interests, security, and the well-being of their societies and people. This includes steps to prevent and counteract the dissemination of terrorist ideologies and advocacy, the financing and training of terrorist attacks, contact among terrorist groups, the spread of manufacturing methods for explosives that are used in terrorist operations, the spread of strife and sedition, and attacks on religions and beliefs (The Arab Convention on Combating Information Technology Offences, 2010). For example, the Riyadh Document stipulates the necessity to punish those who create websites or publish information via electronic networks and other information technologies that facilitate financing and communications between members of terrorist groups, that promote their ideas, or that provide instructions for the manufacture of explosive devices or any other tools that can be used in terrorist acts (The Cooperation Council for the Arab States of the Gulf, 2012).
The UN’s Role in Protecting the Security of Cyberspace from Terrorist Acts


The UN Convention against Transnational Organized Crime (2000) includes articles on international cyberterrorism. These articles clarify procedures for international cooperation to facilitate the exchange of information in fighting electronic terrorism, criminalization, extradition, investigation, and prosecution.

The General Assembly and the Security Council issued several resolutions related to combating terrorism, foremost of which is the United Nations Global Counter-Terrorism Strategy. This discusses strategies and mechanisms that prevent and combat terrorism, as well as maintain respect for human rights and the supremacy of law. The resolution boosts states’ capacities to prevent terrorism and strengthen the UN’s role (The UN Global Counter-Terrorism Strategy, 2006). The action plan includes preventive steps and remedial measures to enhance efforts that address the root causes that drive extremism and terrorism (The UN Plan of Action to Prevent Violent Extremism, 2016).

The UN upholds a set of decisions that strengthen counterterrorism efforts at the international level, including the prevention of cyberterrorism threats. Among its most important decisions is the general assembly’s resolution on the seventh review of the UN Counter-Terrorism Strategy. This resolution encouraged all concerned parties from states, international organizations, civil society bodies, and academia to cooperate in the prevention of terrorist entities from finding an online haven. Its call to strengthen cybersecurity respects the rules of international human rights law. Emphasis was placed on keeping pace when faced with changing and emerging threats of international terrorism represented in the exploitation of information and communications technologies for terrorist purposes (The UNGA Resolution NO. 291, 2021).

The Security Council Resolution 2370 addresses the use of information and communications technologies, particularly the internet, to facilitate the perpetration, incitement, planning, financing, and recruitment of terrorist acts. The resolution encourages governments to develop methods to adapt to evolving terrorist threats (The UNSC Resolution 2370, 2017).

The UN also adopted initiatives to counteract cyberterrorism. These aim to enhance the capabilities of countries to prevent cyberattacks staged by terrorist organizations. Perhaps the most important of these initiatives is the cyber security program, which addresses four axes: (1) addressing the threat of cyberattacks on critical infrastructure; (2) mitigating the spread of online terrorist content; (3) limiting terrorist communications via the Internet; and (4) combating the financing of digital terrorism (The UN Counter-Terrorism Centre, 2019).

It is imperative that we protect the security of cyberspace from threats posed by terrorist activities. However, no legally binding international treaties have been drafted to limit terrorists’ use of cyber weapons. This may be due to the relative modernity of cyberspace, the prevailing convictions among some countries that there is no need for such a treaty, the applicability of previous international texts related to combating terrorism, and the unwillingness of technologically advanced countries to conclude agreements that may restrict their ability to use their own digital technologies.

CONCLUSION

Terrorist groups use emerging technologies in ways that threaten security. Therefore, there is considerable regional and international interest to confront the risks associated with cyberterrorism’s
threats to national security. Terrorist groups increasingly exploit modern technologies to wage psychological warfare to sabotage operations and cause damage and deliberate harm.

Regional and international efforts to combat cyberterrorism have, to a large degree, been effective at preventing terrorists from financing their criminal acts and spreading their ideologies and propaganda. Despite the importance of legal and institutional achievements, there is still an urgent need to confront the significant risks posed by cyberterrorism. In addition, steps must be taken to address risks and prevent cyberspace from becoming an arena for wars and conflicts between states. This includes ways steps to detect and prevent potential attacks.

There are several recommendations to strengthen cybersecurity at the national and international levels.

- Create a binding international agreement to combat cyberterrorism, enhance the ability to deter these crimes, and hold responsible parties accountable.
- Enhance community awareness surrounding cybersecurity, including the seriousness of cyberterrorism. This should be expanded through media by scholars, specialists, and educational, social, and cultural institutions.
- Confront the dangers of cyber activities and issue effective legislative tools to protect cyberspace. Highlight the safe use of information and communication technologies and prevent terrorist or criminal groups from engaging in antisocial practices.
- Develop national strategies to respond to threats from cyberspace. Create international agreements and established laws to confront online attacks.
- Invest in the development of national cybersecurity experts. Encourage research and seminars on cyberterrorism.
- Maintain a balance between liberal democratic norms and effective measures to combat cyberterrorism, ensuring that human rights are not violated. For instance, the fear of cyberterrorism should not be exploited for the unlawful violation of privacy and individual freedoms, especially freedom of opinion and expression. We should not block websites, monitor e-mail, or eavesdrop on electronic communications without evidence of a potential breach of cybersecurity.
- Leverage the expertise of countries that are advanced in the field of cybersecurity. Identify the most effective international strategies to combat terrorism.
- Promote cooperation between interested authorities to reduce threats posed by terrorist organizations through modern technologies (i.e., oversight bodies, judiciary, police, intelligence agencies, technology experts, and the private sector).

ACKNOWLEDGMENT

The author expresses her thanks for the academic and financial support provided by Al-Yamamah University. Special appreciation is given to the reviewers for their constructive comments and suggestions on drafts of the manuscript.

COMPETING INTERESTS

The author of this publication declares there are no competing interests.

FUNDING AGENCY

The publication fees for this research were funded by Al-Yamamah University.
REFERENCES


Defterios, J., & Cavaliere, V. (2019, September 14). Drone strikes knock out half of Saudi oil capacity. CNN.


Gelineau, K., & Gambrell, J. (2019, March 15). New Zealand mosque shooter is a White supremacist angry at immigrants. *Chicago Tribune*.


The UN Counter-Terrorism Centre. (2019, December 10). *Cybersecurity Challenge, Countering Digital Terrorism.* Author.


Maya Khater is an Associate Professor in Public International Law, in the College of Law at Al-Yamamah University, she holds a Ph.D. from the Law Collage at Damascus University in 2011. Before joining Al-Yamamah University, Dr. Maya was working as Lecturer at the College of International Relations and Diplomatic Sciences at Al-Kalamoon University in Syria, then as an Assistant Professor at Dar Al Uloom University, during her career at Dar Al Uloom University, she took many responsibilities; she was the Vice Dean of Admissions & Student Affairs, the Assistant of the Dean’s Collage, and a member of many committees. Dr. Maya has taught many law courses in both Arabic and English languages, she was supervising and reviewed Master’s Theses in Criminal and Commercial Law, and reviewed books and papers for legal journals. In the research area, Dr. Maya has four Books, and she published many research papers in high-ranked journals. The areas of expertise of Dr. Maya are public international law, human rights, international criminal law, and combating international terrorism.