


# 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

9 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: [www.igi-global.com/article/international-perspective-on-securing-cyberspace-against-terrorist-acts/318706](http://www.igi-global.com/article/international-perspective-on-securing-cyberspace-against-terrorist-acts/318706)

## Related Content

---

### A Framework for Managing Big Data in Enterprise Organizations

Youssef Ahmed, Walaa Medhatand Tarek El Shishtawi (2020). *International Journal of Sociotechnology and Knowledge Development* (pp. 84-97).

[www.irma-international.org/article/a-framework-for-managing-big-data-in-enterprise-organizations/242938](http://www.irma-international.org/article/a-framework-for-managing-big-data-in-enterprise-organizations/242938)

### Evaluating the Accessibility of Computer Laboratories, Libraries, and Websites in Jordanian Universities and Colleges

Iyad Abu Doushand Ikdam Alhami (2018). *International Journal of Information Systems and Social Change* (pp. 44-60).

[www.irma-international.org/article/evaluating-the-accessibility-of-computer-laboratories-libraries-and-websites-in-jordanian-universities-and-colleges/199822](http://www.irma-international.org/article/evaluating-the-accessibility-of-computer-laboratories-libraries-and-websites-in-jordanian-universities-and-colleges/199822)

### Paper Rejected ( $p > 0.05$ ): An Introduction to the Debate on Appropriateness of Null-Hypothesis Testing

Mark. D. Dunlopand Mark Baillie (2011). *Human-Computer Interaction and Innovation in Handheld, Mobile and Wearable Technologies* (pp. 323-328).

[www.irma-international.org/chapter/paper-rejected-introduction-debate-appropriateness/52426](http://www.irma-international.org/chapter/paper-rejected-introduction-debate-appropriateness/52426)

### Leadership can bridge the User-Developer gap

David Tuffley (2011). *Knowledge Development and Social Change through Technology: Emerging Studies* (pp. 46-56).

[www.irma-international.org/chapter/leadership-can-bridge-user-developer/52209](http://www.irma-international.org/chapter/leadership-can-bridge-user-developer/52209)

### A Modeling Approach to Simulate Effects of Intercropping and Interspecific Competition in Arable Crops

Heike Knörzer, Simone Graeff-Hönniger, Bettina U. Müller, Hans-Peter Piephoand Wilhelm Claupein (2012). *Societal Impacts on Information Systems Development and Applications* (pp. 160-181).

[www.irma-international.org/chapter/modeling-approach-simulate-effects-intercropping/65009](http://www.irma-international.org/chapter/modeling-approach-simulate-effects-intercropping/65009)