Pakistan Journal of Criminology
Vol. 16, No. 03, July—September 2024 (851-864)

Cyber Attacks and its Implication to National Security: The Need for International Law Enforcement

Jamal Awwad Alkharman[1], Sonia Abed ALhamed Drawsheh[2], Majid Mohammad Al-Khataybeh[3], Zein Bassam BaniYounes[4], Najwa Abdel Hamid Darawsheh[5] & Hanadi Alrashdan[6]

Abstract

Uncontrolled protests championed by Britain and the United States of America increased international interest in cyberspace security. Challenges surrounding cyber-attacks birthed a rethinking to security-concept most especially after the basic values of countless communities have been subjected to risk and threats. Misuse of communication and information technology has extensively led to the collapse of trans-border vital infrastructural facilities. Therefore, the current article came as a rescue to explain how cyber-attacks could be addressed by international law enforcement. The article evaluates the implications of cyber-attacks on national security. It demonstrates how international law could tackle challenges posed by cyber-attacks. The article emphasizes the significance of the cyber security concept to national security strategies; questions the cyber terrorism concept; and analyses how terrorist groups are increasingly using cyberspace for criminal intent. The article further provided solutions after a thorough constructive reviewed of the literature, and concluded that more efforts, control systems, defense systems, and protective devices must be strategically embraced and fixed by international law enforcement agencies. It is believed that the execution of this study's suggestions and recommendations would largely curb and reduce cyber-attack challenges internationally.

Keywords: Cyberspace, cyber-attack, international law enforcement, cyber terrorism.

[1]Assistant Professor, Law Department, Faculty of Law, Jadara University, Jordan. j.alkharman@jadara.edu.io
[2] Psychological counseling, Mutah University, Mutah, Jordan. soniadrawsheh@gmail.com
[3] Department of Curricula and Instruction, Faculty of Educational Sciences, Mutah University, Mutah, Jordan. majid@mutah.edu.jo https://orcid.org/0000-0001-9852-7182
[4] Assistant Professor, School of Arts, Department of English Language and Literature/Translation, Jadara University, Irbid, Jordan. z.baniyounes@jadara.edu.jo ORCID ID: 0009-0001-0150-8426
[5] Department of Educational Foundations and Administration, Faculty of Educational Sciences, Jadara University, Jordan. najwadarawsha@gmail.com ORCID: 0000-0002-0907-2188
[6] Faculty of Education, Jadara University. h.alrashdan@jadara.edu.jo ORCID: https://orcid.org/0000-0001-8898-3117

Introduction

The relationship between security and technology influenced the state's strategic passion for cyber threats, thus making it a modern tool for international multilateral conflict. During the Arab revolution in 2011, social networks played a major role in placing cyberspace security higher at the international level. In other words, cyberspace security became recognized internationally after the emergence of social networks. Therefore, the emergence of social networks on the one hand, and massive protests that occurred in the United States of America and Britain on the other hand, birthed its control against online attacks.

If national security means protection, absence of threat to the basic values of society, and absence of fear of the risk of these values being attacked, cyberspace has imposed a rethinking of security concept, which relates to the degree to which the state can become immune from the threat of attack, and protection measures against the threat to vital infrastructure facilities, through the misuse of information and communication technology (Roztocki & Weistroffer, 2019, Gupta, 2016, darawsha, 2023).

The relationship between cyber-security and national security increases by several reasons. First of all, the increase in the transfer of informational, military, security, intellectual, political, social, economic services. Additionally, the scientific and research content in cyberspace, especially with the acceleration of the adoption of electronic governments and smart cities in many countries leads to such an impact (Qing et al, 2023). The expansion and number of Internet users in the world, and the major revolution in the Internet of Things, where databases of several countries are subjected to external exposure call into questioning its ability to maintain its national security.

Moreover, propaganda campaigns, misleading information, spreading rumors, calling for incitement, or supporting opposition or minorities contribute to the erosion of the state's sovereignty. Accordingly, the countries' passion for cyber security exceeds technical aspects and includes military, economic, social, and other aspects, which worked to support the fact that non-peaceful use of cyber-security space affects the economic prosperity and social stability of all countries that have become dependent on global information infrastructure.

In addition, the escalation of the role of non-state actors in international relations has in turn affected the sovereignty of states, especially with the emergence of the role of transnational technological companies, and the emergence of the dangers of piracy, cybercrime and terrorist groups.

National interests that are linked to critical infrastructure have become vulnerable to attack in cyberspace. These interests are linked to each other in a single work environment. Therefore, any attack on one of these interests is a

reason for a strategic imbalance and a serious threat to national security, and this is what prompted many countries to include cyber-security within their national security strategy. Hence, this article shall focus on weighing the need for international law enforcement amidst cyber-attacks endangering national security (Moon, 1997; Fidler, 2016; Tehrani, 2019, Darawsheh, 2023).

Concept of Cyber Security

The dependence of today's world on information is a fact, and it imposes more reliance on many individuals on electronic systems that cure them. The talk about security calls for defining danger, that is, the threat to which the system is exposed, in addition to weaknesses and loopholes, and then the measures that must be taken to ward off the danger as a result of the increase in threats and risks in cyberspace facing countries, the cyber-security concept emerged (Roztocki & Weistroffer, 2019).

Cyber-security could be described as "the security of networks and information systems, data, information, and devices connected to the Internet. Therefore it is the field that relates to procedures, standards, and protection standards that must be taken or adhered, to confront threats, prevent infringements, or at least limit their effects". Richard Kemmerer defines cyber security as "Thwart the attempts of pirates". While Edward Amorso defined it as "Means that reduce the risk of attack on software, computer hardware or networks, and include those means and tools used in confronting piracy, and detecting and stopping viruses…."(Al-Ashqar, 2012).

Cyber-security can also be defined based on its objectives, as it secures human communication and information resources, and guarantees the possibility of limiting injuries that emanate from threats and risks. Perhaps it will allow the damage not to turn into permanent loss. It is the activity or process, capacity, or information systems and communications of the state, where information is received, and protected from any motive of damage, unauthorized use, explanation, or exploitation. From the practical and procedural point of view, cyber security can be summarized as not exceeding the following concepts such as integrating a comprehensive solution that serves as preventive measures for detecting and thwarting intruders against communication and information hacking that may cause malicious disruption or damage (Schmitt & Thurnher, 2012).

Cyber-security provides solutions to network, computer, and software threats by detecting intrusions, stopping viruses, preventing access, enabling encrypted communications, and enforcing authentication. Cyber-security encompasses guidelines, guarantees, security concepts, policies, treatments, procedures, practices, training, and technologies that could guarantee a safe e-

environment and regulate asset usage (Schulzke, 2018). Cyber security involves a set of measures taken to defend against computer hacker attacks and the obstacles they create. It also includes taking necessary security measures to protect information security against such attacks (Alshaikh &Yousef, 2023).

Through the definitions presented, it can be said that cyber-security prevents any sort of online unauthorized abuse and use of communication and information; restores those abused information and used communication; ensures the functioning and continuity of that information; guarantees privacy and confidentiality of personal data; and taking all preventive and possible means to ensure that consumers and citizens are protected against cyber-risks. Hence, cyber-security could be regarded as a mechanism and strategic tool used by individuals and governments in cyber-warfare as a result of unauthorized interference.

Cyber-security Dimensions

Toward preserving national security and integrating security systems, it is significant to reiterate that political, military, social, economic, and humanity issues are influenced by cyber-security concepts. Therefore, cyber-security dimensions are:

The Military Dimension: The Internet emerged from the military environment, thereafter, it extended to academic and scientific circles. The military uses the internet to monitor war and determine their capabilities over their opponents. The Internet also helped the military in tracking their achievements and developing nuclear weapons (Ridwan, 2016).

One of the benefits of cyber is its capability to connect military units through the military networks in cyberspace, by guaranteeing a convenient exchange of information, and speedy military decision-making which is the achievement of targets from a distance. Undoubtedly, failure to exploit this technology and arm it, or to secure it well from any external penetration, will necessarily lead to launching counter-electronic attacks on the networks of military forces and then destroying the databases and dangers that ensue (Schulzke, 2018).

It can also constitute a point of weakness, especially if it is not well secured from penetration, which may lead to the destruction of military databases, or severe communication between command and military units, as well as the possibility of controlling some weapons and their out of control like drones, guided missiles, satellites, and more (Alshaikh &Yousef, 2023).

The economic dimension: Cyberspace has become attractive to all sectors of society. Knowledge has become the engine of production and economic

growth, and everyone is convinced that the principle of focusing on information and technology is a factor in the basis for economic advancement, which has recently prompted countries to increase their investments in knowledge. Modernization of the economy has become linked to the control of the digital economy by different parties such as economic and social actors (Al-Ashqar, 2012).

Similarly, the use of computers and the Internet in facilitating and developing industries, moving the economy, and processing all economic and financial transactions have become interconnected through computer networks, which call for discussing about the essence of achieving cyber security in the economic field (Al-Ashqar, 2012).

The Social Dimension: It is necessary to generalize the correct and proper concept of security to all participants in the international information network, as it is considered one of the important steps that tighten security if created and developed undoubtedly, and implemented efficiently. Therefore, organizing media campaigns and civic education incorporating risks and challenges, and mapping out deterrent and preventive measures to educate all cyber personnel to deal with the security process is very necessary.

More concentration should be given to individuals, security measures, and deterrent measures including the possible repercussions established under criminal law for failing to respect security architectural designs. Similarly, training and education on communication and information technologies are of great importance. The training should not just focus on deterrent and security measures, but security culture must be inculcated within the culture of information technology (Roztocki & Weistroffer, 2019).

According to the latest statistics, Internet users exceed 4 billion people in the world, of whom more than average use social networking sites, which makes it the largest gathering for human interaction, and opens the door wide for the exchange of ideas and good experiences. However, the monitoring challenges of the content of the internet, on the other hand, exposes society to dangerous morals, subjects identities to external penetration, and thus threatens the peace of society. To attain adequate cyber security in the social dimension, citizens must be educated and enlightened about these risks (Mukhtar, 2015).

The legal dimension: Individual, institutional, and governmental activity in cyberspace entails legal consequences and obligations that require special attention, to settle emerging disputes, and resolve disputes that may arise from them, which requires keeping pace with changes accompanying the arrival of information society such as the right of access to the global network of information, right to create blogs, rights in the establishment of gatherings on the

Internet, and right to information program ownership. Subsequently, modern duties with economic repercussions also appeared, such as the duty to safe contacts, and the duty to report content crimes and violations. All of these changes and transformations require the existence of a legal arsenal that is consistent with the developments taking place at the level of rights, or at the level of environments and processes (Al-Ashqar, 2012).

This is because the rapid technological developments impose keeping pace with legal frameworks designed for lawful and unlawful actions in cyberspace. It is noted that cybercrime in most cases and countries lacks legal frameworks and strict measures to tackle the attacks. In essence, there is a need for joint international cooperation to combat cyber-attacks (Schmitt, 2012).

The political dimension: The various leaks and exposure of sensitive information and documents that caused international and external threats in the political space are leading examples of the political dimension of cyber-attacks. In other words, political secrets are easily visible on social networks during election campaigns, and virtual and electronic demonstrations.

In another context, the use of these sites by terrorist movements to recruit their members and collect financing for their operations must not be overlooked. Using these sites as a mechanism for communication between them as individuals and as groups is what makes it necessary for states to protect their security from threats and risks that may be exposed through the Internet (Mukhtar, 2015). This is in addition to leaks of sensitive documents and breaches that often lead to diplomatic crises between countries. Cyberspace has become a fertile environment for electoral campaigns and propaganda for various international actors.

The Importance of Cyber Security in National Security Strategy

The Deep Web and Dark Web:

Terrorist groups in the world use highly complex and sophisticated digital technologies, starting with the dark web, which makes countries and authorities "Dark Net" (which is considered a means of anonymity), and invisibility finds tremendous difficulty in the source of the threats. Moreover, terrorism is not limited to its presence in hidden sites but has moved to open space or the World Wide Web. In any case, these methods do not differ in their content from those used in organized cybercrime or individual against persons or companies. The dark web is part of the hidden internet (Net Hidden) that cannot be accessed using normal browsers (Navigateur) or search engines (Recherche de Moteur) such as Google and Yahoo or others. For this type of use, there are special browsers such as "TOR", "Freepto" or "FreeNet" and others. The main advantage of these browsers is to hide the trace that can be left by surfers on the Internet and to

prevent the security services from being tracked and monitored. This allows users to protect their identity and information about the source of their communication, create websites on the Internet without revealing the originator, bypass blocking programs that countries use to block some websites and create a safe and invisible network. Confidential information is sent, and this is secured through a technology based mainly on a data encryption system and a network of thousands of distributors around the world, which receive requests to enter the sites, as they are encoded before resending them. This is what secures anonymity of identity and confidentiality of browsing and movement (Schmitt, 2012, Gupta, 2016).

It should also be noted that most of this software was initiated by research projects belonging to the US Navy, in contrast to the Internet, which many mistakenly believe that its origins were directed primarily at military needs, meanwhile, the truth is that it was directed at scientific and research purposes through the Arpanet project (Agency Projects Research Advanced Network) with financial support and funding from the US Department of Defense. It has been developed within universities and research institutions to be a tool for scientists to share scientific materials for non-military purposes. This was intended to secure the privacy of communications and information of the devices connected to it, and then this feature began to be circulated to employees of international organizations, government agencies, and security agencies (Lewis, 1981).

However, it was not too late to reach cyber-criminals. Therefore, terrorist groups as such in general, have been used in drug and weapons trafficking, securing mercenaries, murders, and trafficking in military data and others. However, cyber terrorism has become a public concern through the open internet, as it secures its hostile operations through the dark internet while spreading its ideas on the open internet through social networking platforms and public websites. Security services also face similar difficulties while tracking and tracing arguments on those sites. This occurs because these groups often adopt the hit-and-run approach which makes them disappear and re-appear with different profiles and titles (Trahan, (2016).

Questioning the Concept of Cyber-terrorism

Based on the widely growth of the Internet in all parts of the world, many changes and developments have emerged. Individuals access it, and the emergence of the Internet has become associated with many threats that the world has witnessed through many terrorist groups, for example, the "ISIS" organization and many terrorist organizations. This resulted in the birth of the term "electronic terrorism". The word “cyber terrorism” or “electronic terrorism” was used in the eighties in Collin Barry’s study, in which he indicated the difficulty of defining

the electronic terrorism phenomenon accurately, not to mention the methods and solutions required to confront it, as well as defining the role of computers and the Internet in terrorist action. The term "cyberterrorism" encompasses the tactics, weapons, and objectives of terrorism in intervening in the policies and security of states (Al-Khasawneh, 2022).

James Lewis defined cyber-terrorism as “the use of computer network tools to destroy or disrupt important national infrastructure such as energy and transportation or to intimidate the government and civilians” (Dutton, 1992). The FBI defines cyber-terrorism as “a deliberate, politically motivated attack against information systems, computer programs, and stored data by various actors, which is the threat or unlawful attack of attacks on computers, information systems, programs and data with the aim of intimidating and coercing governments to achieve various goals” (Desforges, 2011). Hence, cyberterrorism refers to the commission of terrorist acts using information technology systems. Therefore it can be considered a new technological tool of traditional terrorism. In this sense, cyberterrorism can transcend national borders and influence countries and societies regardless of phobic geographical location. Similarly, another study posits that cyber-terrorism’s main objective is to attract attention, create panic and fear among the civilian population, and coerce governments into undesirable policies (Abdel Wahhab, 2011).

It can be said that cyberterrorism is the point at which disturbing special cybercrime intersects with cyberspace. In this sense, it differs from cybercrimes, such as data theft, bank fraud, etc. Cyber-terrorism targets people, property, or infrastructure, It leaves varying grades of damages that may lead to death, physical injury, explosions, or severe economic losses, as cyberspace represents an important attraction for terrorist organizations of all kinds and different ideologies, due to what it provides of an international media and as a weapon that can be used by multiple parties from different locations (Al-Khasawneh, 2022)

Objectives of Cyber Terrorism

Cyberterrorism aims to achieve a set of illegitimate goals, among which include achieving safe organizational communication for some elements of terrorist organizations and proving their presence on the scene by broadcasting many terrorist dialogues on sites and forums and using them as propaganda outlets.

Cyber terrorist threats and intimidation by broadcasting through some media materials, in the form of propaganda and advertisement, highlight the strength of these organizations in a way to intimidate any of the collaborators with security services and to attract public attention. Similarly, it is within their

objectives to collect or seize money illegally, kidnap innocent people when lured through online chat into participating in job opportunities, or invite them to attend interesting events where they could be easily and secretly picked up and become hostage.

The cyber terrorist, shortly afterward will demand a huge ransom as a key condition before granting freedom to kidnapped victims in the framework of sourcing liquid cash for financing their terrorist operations (Al-Khasawneh, 2022). Cyber terrorist equally violates information security, destabilize tranquility, destroy information infrastructure, and damage means of communication and information technology, or public and private funds and facilities. Terrorists equally promote psychological warfare, as terrorist organizations may use the Internet for tactical deception, such as filming and killing hostages, which reach all parts of the world (Abdel Sabour, 2014).

The Use of Cyberspace by Terrorist Groups:

Terrorist groups are working to use advanced technology to discharge several sabotage acts through:

1. **Communication**: The Internet is used by these terrorist groups to pass information to their members, fund their activities and operations, and obtain sensitive information.
2. **Spreading extremist ideas**: To use young people for terrorist activities, extremist views, and ideas are spread through chat rooms and social networking sites.
3. **Planning and coordination**: The Internet is the major platform used by terrorist groups to coordinate and plan themselves for attacks.
4. **Electronic indoctrination**: Through electronic means, methods and instructions for making booby-trapping, lethal chemical weapons, and hand grenades are provided.
5. **Electronic Funding:** Terrorist groups receive electronic funding and organize campaigns to collect financial donations, especially with the spread of electronic currencies such as Bitcoin (Al-Ajlan, 2008).

The recruitment of young people is one of the most important characteristics of this type of terrorism, as terrorist groups recruit through the Internet, and use young people to carry out their activities.

These groups announced through their sites on the Internet their need for suicide elements. If they were announcing vacancies for young people, they were being used and indoctrinated in that world aspect, as they always describe the goals that their operations are targeted toward the infidels, and they call the youth

to jihad and urge them to become martyrs for the sake of their creator and unconditional entry into paradise.

From this backdrop, the terrorist organization "ISIS" is considered the most real threat to the safety of the global Internet, using it for propaganda, recruitment, financing, information gathering, coordinating terrorist attacks, and a means to mobilize its sympathizers, who are spread all over in a large number of cities. The terrorist organization "Daesh" uses social networking sites to attract those who do not join the organization to lure them into recruitment and spread its ideology among the youth. Their campaigns through the Internet can sometimes be sufficient to provoke acts of violence, fear, and terror in many countries and societies.

In this context, "Abu Bakr Naji" identifies in his book "Management of Savagery" the methods of employing jihadi media within the strategy of terrorist organizations. In 2015, writer and journalist Abd al-Bari Atwan published a book entitled "The Islamic State... The Digital Caliphate," in which he detailed the electronic strategy of ISIS, "The Islamic State in Iraq and the Levant", and analyzed that strategy in detail. These are chapters from his book, detailing that terrorist organizations took advantage of the chaotic environment that followed the Arab revolutions after 2011.

Aswan believes that the Islamic State organization has three elements of state such as a people, a region, and a government. Abu Bakr Naji, in his book “Management of Savagery”, discusses the modalities of using violence and brutality through stages that eventually lead to building the great Islamic state.

The author also dealt with the methods invented by the organization in the field of cyber or electronic warfare, without which it would have been very difficult to establish an organization of this size in a short period. This is mainly due to its recruitment for digital par excellence generation, and based on the latest technologies in communication or publishing films, or other means of organization in conducting and leading digital war (Al-Ashash, 2018).

Role of International Law Enforcement in Combating Cyber Attacks

A hypothetical scenario for a future war or what is known as cyber warfare is in the form of accurate and highly complex attacks through computer systems, networks, and smart devices, which affect the national security of the state and affect international peace and security, as it targets civil and military infrastructure of countries from power and electricity stations, communication systems, transportation, satellites, geo-location services, self-driving cars, as well as nuclear reactors, dams, and water reservoirs. International law enforcement agencies need to provide informational and logistical support that would penetrate

networks to reveal secrets and hijack strategic economic plans, and their interrelated areas. The agency must ensure they carry out the tasks of both attack and defense, as well as the task of providing support to military units fighting in various fields.

They must carry out the task of attack by attempting to launch attacks, targeting the enemy's command and control systems by disabling air defense systems and missile launchers, controlling autonomous weapons such as military robots, cutting off communication networks between military units, as well as performing deception and digital jamming on enemy devices.

International law enforcement agencies must bear it in mind that it is within their responsibilities to decide whether there has been a breach, or a threat to international peace and security, or if an aggression act has occurred which includes all kinds of threats, regardless of the threat means used in it as long as there is hostile intent. It does not matter whether the method used in the attack is conventional or cyber, but important is the damage that results from the attack, which poses a threat to international Security and State Sovereignty.

In the search for protecting the infrastructure of global information against cyber threats, inclusive initiatives and legislative frameworks that deal with emerging phenomena and national security must be formulated at the regional, national, and international levels. Hence, the idea of international cooperation must determine what could constitute a critical infrastructure, in light of the adoption of strict legal and security measures that can prevent and address threats with non-traditional characteristics, such as the case of electronic attacks.

The struggle of international communities on cyber-attacks has reflected a clear and growing interest on the part of the two sectors such as private and public sectors, in cooperation with each other. Many developed countries have sought to adopt a common strategy toward cyber-security, through several laws such as the International Multilateral Partnership Initiative to Combat Cyber-terrorism (IMPACT), which aims at mobilizing international efforts on the part of government and private sectors to confront the growing threats posed by cyber-attack. The initiative also sought to collect visions and ideas about training and the exchange of experiences, as several websites were established to combat digital attacks and protect cyber security.

Those sites were a meeting point for information security experts and politicians to discuss what cyber-terrorism attack means and ways to confront it with agencies such as the "SITE Intelligence" that specializes in supervising terrorism on the Internet, studying the fundamental sources of terrorists and their intellectual references, translating their speeches, and monitoring terrorist propaganda (Hakim, 2018).

The issue of cyber-attacks has become a national security priority for many countries that rely heavily on technology and communications in managing their internal affairs. The right of the attacked country to respond to a cyber-attack must not deviate from the framework of the United Nations Charter and International Humanitarian Law in terms of necessity and proportionality.

The act of self-defense against cyber-attacks that reaches the status of an armed attack must meet the requirements of necessity and proportionality referred to in Article 51 of the Charter of the United Nations of 1945, as the latter wants the state to adopt their legitimate defense right for the armed attack.

The provision does not specifically state that a particular weapon should be applied in response to attacks against the state. It indirectly implies that the nature of the weapon to be used in attacks will not be used in response to attacks as it has the effect of denying the use of force. This kind of attack will undoubtedly result in a threat to international security and peace.

Conclusion

Through the above study, it becomes clear that the challenges of electronic attacks are certain, because many societies are under siege in a virtual society governed by democracy, freedom, and chaos without borders or restrictions, as it helps terrorist organizations and scammers to build relationships among their members in outer space, far from security control.

This is what the Internet has achieved by dividing the public into groups and small groups with different perceptions and ideologies. Diversity has taken the development of cultural dispersion phenomenon, as a factional media is used to fuel the flames of racial conflicts and develop hatred tendencies among the masses. While the United States uses it to promote capitalism and hegemony, scammers use it for criminal intent, and terrorist organizations use it to promote the Islamic caliphate or global jihad for self-interests.

Talking from the standpoint of sovereignty is no longer possible. Sovereignty in our current era is relative, and cyberspace is the best evidence of that in view of the threats that surround it and affect the national security of all countries, and even the security of individual and society in particular. The magnitude of electronic attack requires international joint cooperation incorporated with legal and security frameworks, but the phenomenon remains broader and more complex than some could imagine, because it is linked to an elastic and invisible field, and the nature of this field is what encouraged the proliferation of cyber-attack, including cyber-terrorism.

The theory of unlawful action can be relied upon as a basis for establishing international responsibility for the crime of cyber-attacks. The risk

theory is excluded due to the illegality of the state cyber-attacks. The cyber-attack is a use of force as a result of its effects compared to the armed attack. They both achieve the same result, and the results of cyber-attacks can be more destructive and dangerous as it rise to the level of conventional attacks.

To curb cyber-attacks, international law enforcement needs to set up a fast and efficient system for international cooperation; exchange information with all relevant international and regional organizations; maintain stored data on the computer system; encourage countries to ensure protection themselves from cyber-attacks by strengthening their investment in electronic security and protecting its digital infrastructure; training of national cadres and various institutions on how to deal with cyber-attacks, confront them and limit their repercussions; as well as spreading cyber awareness in the society.

Acknowledgment

I would like to acknowledge the initial support received from Jadara University under grant number Jadara-SR-Full2023. This support played a vital role in facilitating this research.

References

Al-Ajlan, A.(2008). Electronic Terrorism in the Information Age, *a research submitted to the first international conference on protecting information security and privacy in Internet law*, Cairo, pp. 12-13.

Abdel Wahhab, A. (2011). Electronic Terrorism, *Police Research Center Journal***,** Issue 39, p. 321.

Al-Ashash, I.(2018). Cyberterrorism and the Challenges of States: A Comparative Study with International Conventions, *previous reference*, 12(1), 173-205

Al-Ashqar, M. (2012). *Cybersecurity: Challenges and Requirements for Confrontation, the first annual meeting of specialists in the security and safety of cyberspace*, Arab Center for Legal and Judicial Research, League of Arab States, Cairo, p. 15.

Abdel Sabour, S.(2014). Digital Terrorism: Armed Groups' Use of Social Media, Trends of Events, *Future Center for Research and Studies*, Volume One, Issue 2, p. 87.

Alshaikh, S & Yousef, E. (2023).The Effect of the (COSO) Framework for Internal Operational in Reducing the Risks of Cloud Accounting and the Mediating Role of Cybersecurity in Jordanian Commercial Banks, *Jadara Journal for Studies and Research*, 9(2),79-115.

Dutton, A (1992), *Using the Game Environment in the Study of Communications Policies and Internet Development*, New Jersey.Information Today, 499-517.

Desforges, A.(2011). Cyberterrorism: Which Perimeter? IRSEM Sheet No 11, P. 03.

Hakim, G, (2018). Cyberterrorism and International Security: New Global Threats and Methods of Confrontation, *Algerian Journal of Political Studies*,5(2), 104-116.

Deng, Qing & Yao, Mengjiao & Zhang, Hui & Yu, Feng & Huang, Lida & Ma, Yaping. (2023). *Constructing a cross-field scenario system to aware systemic risk: national security as an example*. Natural Hazards. 120. 1-25. 10.1007/s11069-023-06265-7.

Darawsheh, N. (2021). The Role of University Administration in Enhancing Intellectual Security Among Yarmouk University Students, *Journal of Education and Training Studies*, 9(5),35-51

Darawsheh, N. (2023) The Impact of Cyber Bullying on the Psychological Well-being of University Students: A Study in Jordanian Universities, *Information Sciences Letters*, 12(8), 2757-2768, https://digitalcommons.aaru.edu.jo/isl/vol12/iss8/26

Fidler, D. P. (2016). Cyberspace, terrorism, and international law. *Journal of Conflict and Security Law*, 21(3), 475-493.

Gupta, D. K. (2016). *Terrorism in The Twenty-First Century: Challenges and Policy Conundrum.* In Challenge and Change (pp. 195–224). Springer.

Ridwan, J. (2016). Cybersecurity, a priority in defense strategies, *Army Magazine*, Military Publications Corporation, Issue 630, Algeria, p. 40.

Roztocki, N., Soja, P., & Weistroffer, H. R. (2019). The role of information and communication technologies in socio-economic development: towards a multi-dimensional framework*. *Information Technology for Development*, 25(2), 171–183. https://doi.org/10.1080/02681102.2019.1596654

Tehrani, P. M. (2019). *Cyber Resilience Strategy and Attribution in the Context of International law*. In European Conference on Cyber Warfare and Security (pp. 501-XVI). Academic Conferences International Limited.

Trahan, J. (2016). An Overview of the Newly Adopted International Criminal Court Definition of the Crime of Aggression. *Journal of International and Comparative Law*, 2(1), 63–82.

Al-Khasawneh, F. (2022) Sustainable Organizational Agility within the Framework of Talent Management Dimensions Amid the COVID-19 Pandemic: International Efforts in Combating Cybercrimes. *Jadara Journal of Studies and Research*, 8(1), 176–192

Moon, D. B. (1997). *"Cyber-Herding: Exploiting Islamic Extremists Use of the Internet*." Monterey, CA: Naval Postgraduate School.

Mukhtar, M.(2015). Can countries avoid the dangers of electronic attacks?, Events Trends Magazine, *Future Center for Research and Development*, Abu Dhabi, Issue 6, p. 6.

Mukhtar, M.(2015). *Can countries avoid the dangers of electronic attacks*? previous reference, p. 7.

Lewis, J. A. (1981). Rethinking Cyber Security: Strategy Mass Effect and States.A report of the CSIS Technology Policy Program.Center for Strategic and International Studies.

Schmitt, M. N., & Thurnher, J. S. (2012). *Out of the loop: autonomous weapon systems and the law of armed conflict*. Harv. Nat'l Sec. J., 4, 231.

Schulzke, M. (2018). The politics of attributing blame for cyberattacks and the costs of uncertainty. *Perspectives on Politics*, 16(4), 954–968.