OPEN ACCESS
Scholars International Journal of Law, Crime and Justice
Abbreviated Key Title: Sch Int J Law Crime Justice
ISSN 2616-7956 (Print) |ISSN 2617-3484 (Online)
Scholars Middle East Publishers, Dubai, United Arab Emirates
Journal homepage: https://scholarsmepub.com/sijlcj/

Review Article

Cyberterrorism as a Threat to International Peace and Security: A Critical Discourse

Jamal Awwad Abdallah*, Mohd Badrol Bin Awang, Ph.D, Abdullahi Ayoade Ahmad, Ph.D

Faculty of Law and International Relations, Universiti Sultan Zainal Abidin, Terengganu – Malaysia

DOI: 10.36348/SIJLCJ.2019.v02i10.004 | **Received:** 04.10.2019 | **Accepted:** 11.10.2019 | **Published:** 25.10.2019

***Corresponding author:** Jamal Awwad Abdallah

Abstract

With the end of the previous millennium and the entry of the new millennium, a new and somewhat strange war emerged. With the technological development and the invention of modern computers, this threat has become inevitable and imminent for both big and small countries. The new form of conflict is as challenging to international peace and security as the traditional ones and came with new threats that take place in a virtual battlefield known as cyberspace. Thus, cybercrimes, cyberterrorism and cyberwarfare came under the limelight on the international stage and became one of the primary concern of the world of the United States and other world powers. The western powers started considering cyberterrorism to be same with traditional terrorism and advocate for the application of equal measure to address it. The qualitative descriptive method of data analysis was utilized in making meaning out of the data collected from the secondary sources. It involves a descriptive summary of the information collected on specific events of the issues under study. This paper dwells on the phenomenon of cyberterrorism with inquisition of whether international law applies to cyberspace. Finally, some recommendations are offered on how to address the issue.

Keywords: Cyberterrorism, cyberspace, Cyber-attacks, International peace and Security, International Law.

INTRODUCTION

The term "cyberterrorism" was coined in the 1980s by Barry Collin referring to the usage of cyberspace to perpetrate acts of terror. Though, the word started becoming popular parlance among cybersecurity experts in the 1990's as the information and communication technology was developing and spreading across the globe [1]. Many researchers and pundits have affirmed that cyberterrorism is a grave threat to global peace and security that must be judiciously contained. The defence strategy has to include the virtual world to reduce physical damage in the real world. There are incidents of significant cyberterrorism that occurred in the year 2008, 2012 and beyond and risk associated to the transnational hacking activities of cyberterrorist cannot be underrated due to the destructive impact it could have on nations national security thereby triggering global unrest [2].

The term terrorism is a relative term. As such, there is no universally accepted definition of the concept. There is ambiguity as to what constitutes an act of terror since a terrorist to one party could be a freedom fighter for another. Therefore, so far, there is no undisputed legal or academic definition of the concept [3]. As such, the definition of terrorism is left at the subjective interpretations of states and other actors on the international stage to conform with their interest at a given time for a particular purpose. Thus, concepts such as cyberterrorism that are derived from the term terrorism do not also have a generalised academic or legal definition that is universally accepted [4]. For this reason, cyberterrorism as a concept is mostly described based on the method of attack, the target of the attack, the motivation behind the attack, and the criticality of workstation use in the act.

With the end of the previous millennium and the entry of the new millennium, a new and somewhat strange war emerged. With the technological development and the invention of modern computers, this threat has become inevitable and imminent for both big and small countries. The tremendous scientific growth of the present era did not lead to the manufacture of the new lethal weapons new but invented what is more harmful. Cyberspace has also become the essential safe-haven for extremists and racists, where extremist, terrorist, political, religious, ethnic and personal interests can be broadcasted through the Internet. The attack in the traditional sense

may include the launch of a missile or a shell or a fighter aircraft that targeted the enemy, while the situation is entirely different in the case of Cyber-attack, where it requires a computer, Internet and a user [5].

The Threat of Cyberterrorism to International Peace and Security

The primary body responsible for the maintenance of international peace and security is the United Nations Security Council (UNSC), which is considered the most critical, precise and sensitive organ of the United Nations system. By entering deeply into the details of the United Nations (UN) Charter, Article 2(4) of the Charter prohibits the use of force against other States, whether direct or indirect and considers electronic power to be one of the indirect effects. Thus, one of the principal purposes of the United Nations is to remove anything that endangers global peace and security and to ensure the compliance and respect of international agreements by states and non-state actors. In the contemporary world order, resorting to the use of force in international relations should be the last resort [6].

When we talk about weapons and soldiers, we immediately imagine carrying conventional weapons, and a soldier with a gun to fight and enter enemy positions. But here our subject is entirely different from what happens in a traditional war. Cyber fighters and cybercriminals have a very high level of experience in dealing with electronic equipment that is above and at least equal to security systems, and this experience can interrupt communication of control systems, invade banking systems, disrupt civil aviation, hijack electronic voting, and other vital matters. So we get to the basic rule that those who make cyber-attacks are ordinary people, but these people have tremendous experience and very sophisticated capabilities, as they can attack and cause damage from any location in the world [7].

After the events of September 11, 2001, the world turned to a new type of destruction and undeclared wars to the so-called terrorism, which relied on deception, but the attack of information security was one of the most prominent characteristics, so that the attackers relied on access to electronic networks before they began any practical step, so they worked to track the air traffic and penetrate the security systems and then they issued passports and false cards that distract the authorities from any doubts about their terrorist intentions [8]. Terrorist cyber-attacks are modern ways that need only using a computer's keyboard, which highlighted the phenomenon of attacks on the WikiLeaks site where the Anonymous group made hacking operations on a global scale. This group is one of the most influential groups in modern-day piracy, whose number is unknown, or who they belong to. The most famous operations of this group were their support of WikiLeaks [9].

This group has caused many political problems in the world in addition to their attack against several international companies and their intervention in the Iranian elections in 2009, with their offensive against Australian government sites in order to allow the user to browse any site freely, in addition to government sites of many countries and leaked personal information of famous personalities in Bahrain, Morocco, Egypt and Jordan. The Arab Spring was an intensive field of work for members of this group, providing instant support to the popular revolutions in Tunisia and Egypt by launching active attacks against the government sites of the two countries. Some praised them as professional fighters and others condemned them as chaotic computer fighters [10].

Accordingly, it is concluded that the first cyberspace soldiers are those hackers who rely on cyberspace to carry out their terrorist attacks on sites and countries. We remind the revolutions that took place after the Arab Spring, where this group has used Facebook revolutions, as they monitor of their computers aimed at overthrowing political regimes. They sought to overthrow the political systems and succeeded in the Arab Spring revolutions and achieved their goals [11].

The first types of weapons used by these cyber terrorists are hacking. Hacking information systems has become easy under rapid technological advancement. Cyberterrorists can send a message that would harm their victims by e-mail. The attack on Saudi Aramco is a real example of this. It is considered one of the strongest attacks on large companies of this kind. After searching and investigation, it was found that the planning of this attack was organized by an organization outside Saudi Arabia and several countries. The virus was immediately isolated, prevented from entering its networks and additional protection measures were put in place for any future similar attack. The aim was to stop the flow of oil and gas to the world and stop production altogether [12].

When searching for details based on a report issued by the Saudi Ministry of the Interior, the penetration was reported as a result of the virus being planted through a process called "phishing". The operations took place during a month or more of the failed attempts until they reached the discovery of weaknesses in the company's electronic system. The company confirmed that the source of the attack was external, as the result of the penetration of virus planting and encircling the company's security programs and destruction of anti-virus programs and scan a file on each device. This attack was followed by another attack called "dumping" to direct massive operations at the same time and from different parts of the world and led to a temporary interruption in the company's delivery of its services. This attack is

believed to have been aimed at diverting attention from the main attack. Within one day it was controlled and the devices returned to immediate action. However, the effects continued for several months until the company was able to restore the status quo. Electronic attacks threaten 69% of Saudi companies [13].

Based on the Jordanian Electronic Transactions Law in Articles 37 and 38, it states that the Jordanian legislator has imposed severe punishment on anyone who penetrates electronic economic systems, discloses secrets or provides incorrect information about clients and institutions. In addition to the penetration there are many other weapons used by the perpetrators of cyber-attacks including, viruses, worms, Trojans, and dumping. Through these fraudulent tactics, cyber attackers enter the systems to destroy what they can ruin [14].

When we look at these methods, it becomes clear to us that they are lethal weapons that harm their victims. When a particular virus or Trojan horse is spread, a virus term through its name becomes apparent to us that it is a subtle and invisible thing. That is a hidden program or hidden tool that has harmful effects and is effective during cyber-attacks and causes paralysis and disruption of systems [15]. As well as when talking about Trojan horse as the story of this horse includes that a real process of mobilizing soldiers inside the body of a large horse to penetrate one of the fortresses in ancient times and sneak into these fortresses on the basis that it was presented as a gift to one of the rulers at the time. The idea of Trojan horse in cyber-attacks is based on the same principle as it penetrates the systems in a friendly way and enters as a friend or ordinary and ineffective program. When it opens, it transmits several viruses that lead to leaks of data and disclosure of secrets to any person or government entity that enters into its account [16].

Therefore, all member states of the United Nations are sovereign and equal to the international system. Through the recognition and sovereignty of all independent states, which deal with all the subjects of international law and are at the forefront of the United Nations principles in building their relationship with member states. Some scholars believe that cyber-terrorist attacks are equivalent to armed attacks and that they are an issue related to self-defence and long-term political interest. The national and global interest is concerned with the cause of international security and stability. Terrorist cyber-attacks threaten the protection and stability of all countries of the world [17].

Rationally, it is believed that when a terrorist attack a member state of the United Nations, the Security Council must take appropriate measures and effective measures to deter this attack. It should be noted that the text of article 39 of the UN charter did not set a specific definition of aggression, but left it extended so that the Security Council can adopt any action that would endanger the safety of states. Thus, cyber-attacks can be placed under this item, because if we leave things on the contrary, countries will be vulnerable to electronic piracy and attacks and an easy tool controlled by the major powers of the advanced world, which makes less developed countries vulnerable to dangers and tampering with their electronic infrastructure [18].

CONCLUSION

In sum, cyberterrorism threatens international peace and security. Legally, it is a violation of the principles of the United Nations. States have the right to control the space infrastructure and space activities in their territories and to protect their territories from harmful acts through their sovereign right. Therefore, the legal procedures and principles of cyber-attack must prevent the parties to the international relations from using force against territorial integrity, political independence or any other situation that is incompatible with the purposes and principles of the United Nations [19]. As such, all states members of the United Nations are equal regarding sovereignty and in terms of the subjects that deal with international law and deserve to be protected. Some scholars believe that cyber-terrorist attacks are equivalent to armed attacks and that they are an issue related to self-defence and long-term political interest. The national and international interest of many states and non-state actors is concerned with the global peace, security and stability, and Cyberterrorism threatens this interest which in turn affect the stability of countries around the world [20]. Finally, the stipulation of an international legal instrument is recommended where all member states of the United Nations and influential non-state actors must be signatories.

REFERENCES

1. McCarthy, D. R. (2015). *Power, information technology, and international relations theory: The power and politics of US Foreign policy and internet*. Palgrave Macmillan.
2. Valeri, L., & Knights, M. (2000). Affecting trust: terrorism, internet and offensive information warfare. *Terrorism and Political Violence*, *12*(1), 15-36.
3. Ramsay, G. (2015). Why terrorism can, but should not be defined. *Critical Studies on Terrorism*, *8*(2), 211-228.
4. Vertigans, S. (2015). "Terrorism," in International Encyclopedia of the Social & Behavioral Sciences: Second Edition.
5. Schmidt, A. V. (2016). Cyberterrorism: combating the aviation industry's vulnerability to cyberattack. *Suffolk Transnat'l L. Rev.*, *39*, 169.
6. Astrada, M. L. (2017). Security, Law & Public Policy-Assessing the Efficacy of a National Security vs. Law Enforcement Model to Combat Terrorism. . *Thomas L. Rev.*, *30*, 180.

7. Mselle, L., Mrutu, S., Raisi, R., & Kondo, T. (2018). The Word mobile phone Missing in the Cyber Crime Act, 2015. *Journal of Informatics and Virtual Education (JIVE)*, *1*(5), 1-6.
8. Matthews, J. (2015). Framing alleged Islamist plots: a case study of British press coverage since 9/11. *Critical Studies on Terrorism*, *8*(2), 266-283.
9. Hunt, E. (2019). The WikiLeaks Cables: How the United States Exploits the World, in Detail, from an Internal Perspective, 2001–2010. *Diplomacy & Statecraft*, *30*(1), 70-98.
10. Schulzke, M. (2018). The politics of attributing blame for cyberattacks and the costs of uncertainty. *Perspectives on Politics*, *16*(4), 954-968.
11. Arafa, M., & Armstrong, C. (2016). " Facebook to Mobilize, Twitter to Coordinate Protests, and YouTube to Tell the World": New Media, Cyberactivism, and the Arab Spring. *Journal of Global Initiatives: Policy, Pedagogy, Perspective*, *10*(1), 6.
12. Vishwanath, A. (2016). Spear Phishing: The Tip of the Spear Used by Cyber Terrorists. In *Combating Violent Extremism and Radicalization in the Digital Era* (pp. 469-484). IGI Global.
13. Kshetri, N. (2016). Cybersecurity in Gulf Cooperation Council Economies. In *The Quest to Cyber Superiority* (pp. 183-194). Springer, Cham.
14. Tubaishat, B. M. (2019). The Legal System of Electronic Check in Jordanian Law. *JL Pol'y & Globalization*, 85(12), 145-161.
15. Tsagourias, N. (2017). The Law of Cyber Warfare: Restrictions, Opportunities and Loopholes. *Canadian Journal of Law and Technology*, *15*(1), 34-52.
16. Bellovin, S. M., Landau, S., & Lin, H. S. (2017). Limiting the undesired impact of cyber weapons: technical requirements and policy implications. *Journal of Cybersecurity*, *3*(1), 59-68.
17. Luca, G. (2017). Manifestations Of Contemporary Terrorism: Cyberterrorism. *Research and Science Today*, *13*(1), 20-25.
18. 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.
19. Kovalenko, K. E., Rozentsvaig, A. I., & Gubareva, A. V. (2018). International terrorism and international cyberterrorism. *Revista QUID*, *1*(2), 125-128.
20. An-Na'im, A. A. (2016). The spirit of laws is not universal: Alternatives to the enforcement paradigm for human rights. *Tilburg Law Review*, *21*(2), 255-274.