Doi Number :http://dx.doi.org/10.46872/pj.84

CYBER TERRORISM: A POTENTIAL THREAT TO GLOBAL SECURITY

Jobin Sebastian
Annamalai University, Faculty of Arts, Department of Political Science and Public Administration, Chidambaram, India
Dr. P. Sakthivel
Annamalai University, Faculty of Arts, Department of Political Science and Public Administration, Chidambaram, India

Abstract

A large portion of the average folks across the world is unconscious about the menace of cyber terrorism. Today cyber terrorism has emerged as a potential threat to the very existence of sovereign states and thrown challenges to national as well as international security. Most of the developed and developing nations are well-outfitted measures to tackle any challenges from conventional terrorism. In the era of technocracy, ICT enabled devices and services such as computer, mobile phones, social media, etc. have become perfect tools to wage neo or cyber warfare with democratically elected governments all around the world. Even in the amidst Covid–19 pandemic situation, Data theft, breaching of privacy of individuals, unauthorized access to Covid-19 related health research, virus attacks, ransomware attact etc. are penetrating every day. By cyber terrorism, the terrorist can crush the whole digital administration and financial arrangement of a nation. Now it has become a compulsion that, most of the countries especially developed and developing countries are investing more money for strengthening their cyber security system.

The wide use of cyberspace for communication, administration, business etc. and lack of cyber security awareness made the alarming growth of cyber terrorism. Besides, the lack of uniform and strong international rules and regulations and lack of modification of existing rules dangerously help cyber terrorism. This paper attempts to comprehend the development of cyber terrorism and how it has posed challenges or potential threat to global security.

Key Words: Cyber Space, Cyber Security, Cyber Terrorism and Global Security

Introduction

National security is a prime concern of every nation. Today, almost all the nations pay key attention to ensure national security as well as cyber security. Terrorism is the major threat to national security. Among various types of terrorism, cyber terrorism has become a real threat to global security. In the age of Information Technology, the cyber terrorists are using the new technology as a weapon to commit crimes against governments, individuals, business, etc. without any border and they result in irrevocable and terrible damage to the nations. Cyber terrorism and global security became and are becoming the allied terms in the present world and cyber terrorism holds a major share of the security threats in the world. The alarming growth of cyber terrorism is visible from the various reports of nations. Terrorist exploits the growth of technology and attacks the entire system of a nation within a point of time.

Most of the individuals are the victims of cyber crimes knowingly or unknowingly. No one is free from it because the present day life is closely related to the cyber space. Day to day communication, business, administration, etc. are very much depended on cyber space and these make cyber terrorism very easy. In cyber terrorism, the terrorists are using various types of cyber crimes such as data theft, ransomware attacks, spread of virus, hacking and spoofing of government websites, unauthorised access, etc. to wage war against democratically elected governments

across the world. By using the available technology the terrorists can destabilise the security system and the entire infrastructure of a nation and it may lead to potential loss in terms of financial, mental agony to individuals as well as policy makers. To accomplish their objectives, the terrorists attack the computer systems that control air traffic, electric power grids, telecommunications networks, military command systems and financial transactions (Hani and Rajan 2018). These types of attacks are going on in the cyber space at national and international level.

The terrorist are using the best time and best technology to exploit the cyber space. This is very clear from the official news of the INTERPOL. According to the news, cyber criminals are exploiting the uncertainty and fear of the individuals in the midst of Covid-19. First four months of 2020 itself reported 907,000 spam messages, 737 incidents related to the malware and 48,000 malicious URLs related with the Covid-19 ('INTERPOL Report Shows Alarming Rate of Cyber attacks during COVID-19' 2020). This shows the alarming pace of the cyber attacks.

Most of the nations have their cyber security measures. For instance, in India the union government enacted Information Communication Act 2000 and IT Act 2008 which covers the individuals from any kinds of human rights violations in the internet world. In addition to domestic laws, there are some global level structures are available to prevent cyber terrorism. But sometimes these measures are not enough to combat cyber terrorism. The major reason behind this is the technological up hand of terrorists in using the technology cyber space. In other words, the terrorists and their most of the times the nations are equipped with the combating measures only after the attacks. Besides, the lack of strong international level rules and regulations regarding the cyber space help the terrorist. Due to this reason, the affected nations are not able to take proper actions against the international cyber criminals. The boundary less attacks in cyber world is a threat to global security.

Objectives

1. To illustrate types of cyber terrorism and causes for its eruption at the global level.
2. To elicit the need for dynamic international cyber laws to prevent cyber terrorism and to ensure global security.
3. To unearth the global level combating measures to deal with cyber terrorism.

Methodology

This paper adopts the document and analytical method. A major chunk of the literature was collected from articles published in research journals, newspapers, weeklies, fortnightly magazines, government reports and study reports by cyber security agencies and investigation agencies etc.

Cyber Terrorism-A Global Threat

The alarming growth of cyber terrorism as a global threat is beyond our expectation. It is widely believed that, the present and future generations are going to be victims of high-tech terrorism, the cyber terrorism. According to the annual cybercrime report by CyberSecurity Ventures, cybercriminal activity is one of the biggest challenges that humanity will face in the next two decades (Morgan 2019). The reasons behind the vulnerability in the cyber space are the wide use of the cyber space and the lack of security awareness. The day to day communication, business, administration, etc. are closely related to the cyber space and at the same time, they are not well protected by security measures. These have further fuelled the growth of cyber terrorism. While analysing the cyber terrorism, we can see different types of

cyber attacks such as ransomware attacks, hacking, spreading of malicious software etc.

Ransomware is the malicious software that can attack the entire computer system and the restoration of the system demands a huge amount of ransom. By this cyber terrorists are attacking the computer system of the government and other organizations by exploiting the limitations of the security system. By this attack, the system cannot be operated and it restricts the access to the files. This is installed in the system through links in mail, messages, etc. The growth rate of ransomware attacks is increasing every year. According to Cybersecurity ventures, in 2019 the ransomware attack occurred every 14 seconds and it will be in every 11 seconds by 2021 which was in every 40 seconds in 2016 (Morgan 2019). WannaCry was ransomware in 2017 and it affected almost 150 nations and the global impact of this attack was around $4 million in worldwide ('what are the different types of Ransomware?' 2020). The Ransomeware attacks are in increased rates at the time of Covid-19 pandemic. Cybercriminals are targeting the hospitals, medical centres and public institutions since they are overwhelmed with the pandemic issue and cannot afford to take the security of their system. The ransomware can enter their systems through emails containing infected links or attachments, compromised employee credentials, or by exploiting vulnerability in the system(Sakthivel 2020). According to the report there is a growth of 148% in the ransomware attacks related with covid-19 pandemic (Hardcastle 2020).

By hacking the terrorists attempt to exploit a computer system and to gain data by unauthorised access for some illicit purposes. Here the hackers are exploiting the unprotected data and poor cyber security. They can use the hacked data for financial gain and social exploitation. The hackers try to disturb the nation and individual by attacking the virtual world around them but it affects the real world. They attack government and private websites to miss guide the people or to demand ransom or to steal data. The hackers can attack the whole government-related websites, especially which are related to national security. The hackers are very active in the wake of Covid–19. There are numerous researches are being conducted all around the world to develop vaccination to fight against the pandemic. The Hackers lure to setting up fraudulent internet domains, promised to supply masks and medical relief materials and types of equipment, and then deliver fraudulent loans, extortion etc. Most of the enterprises are allowing employees to work from home and hackers exploit the technical failure and the situation. According to the newspaper report the number cyber-attacks increased more than 200 % at the time of covid-19 (Haritas 2020). This is very much clear from the situation in Canada. Recently, thousands of government accounts were hacked in Canada (*The Hindu* 2020b).

By hacking and use of spyware, the terrorists and the counter nations can access the data of the citizens and they can be used for the destruction of a stable government, disturbance in the government and even they can be used to influence the elections of a state. The issue related to the spyware Pegasus and the ban of TikTok are occurred due to the concern about the data of the citizen. By using the modern technology of artificial intelligence the terrorists or the counter country can analyze the data of the citizen and can influence their social and political life (Roy 2019). Even some of the countries, especially the Australia, have banned the Chinese companies from providing 5G network services, citing national security concerns. It is significant to note here that, though India allowed Chinese firms to participate in the 5G trials but with the current border standoff in Ladakh, there are reports India may take a tougher stand (*The Hindu* 2020a). The UK government had already taken a tough stand

against some of the Chinese companies, especially Huwei, fear of breaching of security of the nation by these companies.

The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) have already given warning to the health care organization and research institutes related with the Covid-19 about the chance of hacking. Besides, they asked them to maintain dedicated cyber security('FBI Urges Vigilance During COVID-19 Pandemic' 2020).

Along with the ransomware attacks and hacking the cyber terrorists are using the cyber space for the spread of terrorism. By false and hate propaganda through social media and other virtual platforms the terrorist groups are brainwashing and recruiting people from different nations. Hate and false propaganda lead to communal violence and religious fanaticism and ultimately lead to traditional terrorism. The ISIS terrorist group is using the social media platform for the promotion of terrorism by providing false motivation for Jihad and Caliphate. By this promotion, they are aiming the young people and recruiting them to the terrorist groups. There are more than forty-five cases of pro-ISIS activities, ranging from online propaganda to travelling abroad to join the Islamic State, recorded in Kerala a state in India itself (Taneja 2019). Even during the time of covid-19 criminals are spreading hate speech and misinformation related with the pandemic and creating thousands of new sites every day to carry out spam campaigns, phishing or to spread malware (Sakthivel 2020).

Eruption of Cyber Terrorism

The cyber world is wide open and every day the number of users is increasing. Almost 4.7 billion people are using cyber space for communication, financial transactions, business, government services, etc. It is around 59% of the entire population (Clement 2020). Cyber users in 2015 were 2 billion and it will be 7.5 billion in 2030 (Morgan 2019). Government services, data collection, data storage, national security system, etc. of the present world are depended on cyber space. This wide use is one of the major reasons behind the growth of cyber terrorism. Lack of security measures is closely related to the wide use of cyber space. The activities of citizens and government sometimes are not properly protected by effective security measures. Most of the cyber terrorist attacks are happening due to poor security measures.

Lack of proper awareness is another reason for the growth of cyber terrorism. Most of the common individuals and government officials are not aware of the vulnerability in the cyber space and they share their personal data and information. Even the daily users of cyber space are not well aware of the threats in cyber space as well as the need for security (Zwilling et al. 2020). Besides, the absence of updated laws and regulations leads to the growth of cyber terrorism. In India, the cyber laws are based on the Information Technology Act 2000 and its amendments in 2008. Likewise while analysing the cyber laws of the nations there comes a gap in the timely amendment of the cyber laws and proper implementation of cyber laws ('Global Mapping of Cyber laws Reveals Significant Gaps despite Progress' 2015).

The absence of the experts in the field of policymaking and investigation brings back the combating measures. Most of the cyber experts are working in private sectors but most of the cyber terrorist attacks are happening in the government sectors and if there is a joint venture between the public and private sector, the combating measures will be powerful and successful (Boland 2008). Besides, the public sector should use ethical hackers to understand the insecurity of the system and programme. This will help to update the security measures.

At present, the major reason for the growth of cyber terrorism is the absence of collaboration in a global level (Mendoza 2017). Most of the cyber terrorists are

operating from the foreign nations and the cyber laws of the nation may be different from the affected nations. So that it is very difficult to take proper actions against the terrorists.

Global Level Combating Measures

Most of the nations have their own combating measures to deal with cyber-terrorism. As a global threat cyber terrorism cannot be prevented only by the domestic measures. There should have joint ventures of different nations, private sectors and non-governmental organizations to deal with cyber-terrorism as the vulnerability in any region will affect globally. The world must collectively recognize the challenges posed by terrorists in cyberspace, and update and strengthen national and international policies accordingly (Obama 2011).

The International Multilateral Partnership Against Cyber-Terrorism (IMPACT) is a global organization of different countries and private sector which aims to fill the gaps it finds in security and defences by becoming more proactive toward global cyber-terrorism rather than reactive. It is the first United Nations-backed cyber security alliance. It includes an aggregated warning system which provides accurate information to the nations to prevent attacks. Further, it gives the warning to prevent a local problem from becoming a global problem. Other major initiatives from the IMPACT are the Global Response Centre, Training & Skills Development, Security Assurance & Research and Centre for Policy & International Co-operation (Boland 2008).

The European Union Agency for Cybersecurity, ENISA is a common platform of the European Union to defend cyber terrorism and to ensure cyber security. It was established in 2004 and strengthened by the EU Cyber security Act. It helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness-raising, the agency works to keep Europe's society and citizens digitally secure. It also tries to foresee the cyber security threats in Europe and find solutions and share them to address emerging challenges ('About ENISA - The European Union Agency for Cybersecurity' 2020).

NATO (North Atlantic Treaty Organization) also takes common steps to secure the cyber space in the allies by information sharing and mutual assistance in preventing cyber attacks. The main aims of NATO's cyber defence are crisis management and cooperative security. NATO ensures cyber security by cyber education, training and exercise. NATO Cyber Rapid Reaction Teams is ready to assist the allies to deal with cyber terrorism. From 2016 onwards the cyber defence of NATO is cooperating with the European Union in the area of information sharing, training, research and exercise ('Cyber Defence' 2020).

INTERPOL (The International Criminal Police Organization) plays a major role in securing cyber space. It is an international level inter-governmental organization that helps worldwide police in crime control. As a global threat cyber terrorism is operated usually from the foreign nations and the domestic cyber security measures are not effective to deal with them. So that INTERPOL helps the member nations to combat the international cyber-terrorism by identifying such crimes and coordinating the response to them. It coordinates transnational cybercrime investigations and operations. INTERPOL, by collaborating with the private experts in cyber space, forms a Cyber Fusion Centre to gather information related to cyber threats and to report them. These reports help the nations to be alert against the coming threats. It also coordinates skill development and training against cyber terrorism. Further, INTERPOL gives up to date information and warning regarding cyber security to the nations ('Cybercrime' 2020).

Dynamic International Cyber Law need of the hour

"We must come together now, and we must do it fast, to mitigate this threat and ensure that new technologies remain a force for good rather than a force for evil"[1]. These words by Mr. Vladimir Voronkov denote both the need and scope of international cyber law. As the cyber space is inseparable from daily life and cyber terrorism is increasing globally there should have international rules and regulations. The domestic cyber laws of different nations are not proficient to deal with the international level terrorist.

The borderless nature of cybercrime challenges the domestic law enforcement agencies in responding effectively. The promulgation of such law can implement large-scale regulatory frameworks, reduce security incident, prevent cyber crime, and establish a culture of cyber security (Mendoza 2017).

The Convention on Cybercrime (Budapest Convention) is the first international treaty seeking to address cyber crimes. It was led by European countries and it was established in 2001. It aims to follow a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation, harmonizing national laws, improving investigative techniques, and increasing cooperation among nations ('Convention on Cybercrime' 2020). This transnational convention ensures cooperation in cyber laws and regulations among the member states. Besides, the member states help each other by cooperation in capacity building and mutual assistance. This is an example of international level cooperation in cyber laws. Further, this highlights the scope too.

Even though international cyber law is the need of the time, the promulgation of such law will be very difficult because of the various domestic rules regarding the act of privacy, copyright, etc. To have a common law there should have treaties like the treaties regarding arms control. Besides, when a law is promulgated regarding the cyber terrorism it should be clear about the cyber-attacks from states and non-state actors (Schjolberg and Ghernaouti-Helie 2009 & O'Connell, Arimatsu, and Wilmshurst 2012)

Conclusion

Cyber terrorism is a reality to be accepted. The state, and individuals are affected by the threats in the cyber world and the pace of cyber terrorism is increasing day by day. By different cyber crimes the terrorists wanted to subjudicate or suppress the security network and financial system of governments and makes harm to the vital data, including covid-19 health related issues. This cyber terrorism, a global phenomenon which is a real threat to global security and no state is free from it. National and international combating measures are cooperating to prevent cyber terrorism and trying to have an international level policy to combat cyber terrorism effectively. The global nature of cyber terrorism demands an international cyber law to combat threats in cyber space.

At the same time, international countermeasures and law enforcement alone cannot provide a secure cyber space. There should have a proper cyber culture as well periodical cyber security audit by both government and private officials. This culture can be formed by regular education and awareness to the public about the ethics to be kept in cyber space and about the vulnerability and threats in it. The nations should update domestic cyber laws and encourage '*Ethical Hackers*" to combat the menace of

[1]Remarks by Mr. Vladimir Voronkov, Under-Secretary-General of the United Nations Office of Counter-Terrorism, Side-Event on Countering Terrorism with New and Emerging Technologies, 26 September 2019

cybercrimes effectively. The collaboration between government and the private sector can ensure the effective functioning of the domestic countermeasures. Countermeasures should be able to foresee the threats and act accordingly to prevent them. Further, regular auditing and proper adoption of security measures can ensure a secure cyber space. Hence, by prevention, awareness, implementation of the law, coordination among state and non-state actors, etc. in cyber space can combat cyber terrorism, the potential threat to global security.

References

'About ENISA - The European Union Agency for Cybersecurity'. 2020. ENISA. 2020. https://www.enisa.europa.eu/about-enisa.

Boland, Rita. 2008. 'Countries Collaborate To Counter Cybercrime'. *Afcea*, 1–7. https://www.afcea.org/content/countries-collaborate-counter-cybercrime.

'Cyber Defence'. 2020. North Atlantic Treaty Organization. 2020. https://www.nato.int/cps/en/natohq/topics_78170.htm.

Clement, J. 2020. 'Global Digital Population as of July 2020'. https://www.statista.com/statistics/617136/digital-population-worldwide/.

'Convention on Cybercrime'. 2020. Council of Europe. 2020. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

'Cybercrime'. 2020. INTERPOL. 2020. https://www.interpol.int/en/Crimes/Cybercrime.

'FBI Urges Vigilance During COVID-19 Pandemic'. 2020. FBI. 2020. https://www.fbi.gov/coronavirus.

'Global Mapping of Cyber laws Reveals Significant Gaps despite Progress'. 2015. United Nations Conference on Trade and Development. 2015. https://unctad.org/en/pages/PressRelease.aspx?OriginalVersionID=238.

Hani, Mathiha Nehla, and Aswathy Rajan. 2018. 'A Critical Study on Cyber Terrorism with Reference with 26 / 11 Mumbai Attack'. *International Journal of Pure and Applied Mathematics* 119 (17): 1617–36. http://www.acadpubl.eu/hub/.

Hardcastle, Jessica Leons. 2020. 'Ransomware Attacks Spike 148% Amid COVID-19 Scams'. Sdxcentral. 2020. https://www.sdxcentral.com/articles/news/ransomware-attacks-spike-148-amid-covid-19-scams/2020/04/.

Haritas, Bhragu. 2020. 'Hackers Begin Exploiting Covid-19 Situation at Enterprises'. The EconomicTimes. 2020. https://cio.economictimes.indiatimes.com/news/digital-security/hackers-begin-exploiting-covid-19-situation-at-enterprises/74839021.

'INTERPOL Report Shows Alarming Rate of Cyber attacks during COVID-19'. 2020. INTERPOL. 2020. https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19.

Mendoza, Miguel Angel. 2017. 'Challenges and Implications of Cyber security Legislation'. *Trends 2017: Security Held Ransom*, 43–47. https://trends.fjordnet.com/trends/.

Morgan, Steve. 2019. '2019 Official Annual Cybercrime Report next Two Decades'. https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf.

O'Connell, Mary Ellen, Louise Arimatsu, and Elizabeth Wilmshurst. 2012. 'Cyber Security and International Law'. London.

https://www.chathamhouse.org/sites/default/files/public/Research/International Law/290512summary.pdf.

Obama, Barack. 2011. 'International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World'. Washington, DC.

Roy, Prasanto K. 2019. 'Weaponising Data, the New Oil'. *India Today*, November 2019. https://www.indiatoday.in/magazine/cover-story/story/20191118-weaponising-data-the-new-oil-1616598-2019-11-08.

Sakthivel, P. 2020. 'CYBERCRIMES DURING COVID – 19 PANDEMIC'. *Mukt Shabd Journal* IX (V): 3506–13.

Schjolberg, Stein, and SolangeGhernaouti-Helie. 2009. *A Global Protocol on Cybersecurity and Cybercrime*. Stein Schjølberg and SolangeGhernaouti-Hélie.

Taneja, Kabir. 2019. 'God's own Khilafat? Why Kerala is a Hotspot for ISIS in India'. *The Print*, 21 November 2019. https://theprint.in/pageturner/excerpt/god-own-khilafat-why-kerala-is-isis-hotspot-in-india/320945/.

The Hindu. 2020a. 'Australia Shares Experience on 5G', 14 August 2020. https://www.thehindu.com/news/national/boost-to-cybersecurity-ties-says-tara-cavanagh/article32347379.ece.

———. 2020b. 'Thousands of Canadian Govt.Accountshacked', 17 August 2020.

https://www.thehindu.com/news/international/thousands-of-canadian-government-accounts-hacked/article32369557.ece.

'What Are the Different Types of Ransomware?' 2020. Kaspersky. 2020. https://usa.kaspersky.com/resource-center/threats/ransomware-examples.

Zwilling, Moti, GalitKlien, DušanLesjak, ŁukaszWiechetek, Fatih Cetin, and HamdullahNejatBasim. 2020. 'Cyber Security Awareness, Knowledge and Behaviour: A Comparative Study'. *Journal of Computer Information Systems*. https://doi.org/10.1080/08874417.2020.1712269.