Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

The Need of Strategic Response to Mitigate the Risk of Cyber Terrorism and Maintain International Peace

Dr. Omkar Sunil Sonawane*

* Savitribai Phule Pune University, India

ARTICLEINFO

Received: 05 Nov 2024

Revised: 15 Dec 2024

Accepted: 25 Dec 2024

ABSTRACT

Economic and social peace is an important factor for any nation. However, for a decade, it has been observed that digital platforms are used by unethical people around the globe. Cyber terrorism is an interwoven border where fraud attempts are considered as a base to target people and government bodies. The intention behind it is noted as the disruption of the social, political, and economic status of any country. National security can be counted in terms of the national peace index. Around the globe, many countries are facing terrorist activities as a physical presence of unstable bodies. However, apart from the historical physical attacks, the frequency of cyber terrorism activities is recorded more. Accordingly, it is important to suggest a mitigation strategy for such attempts of cyber terrorism. Computational security is an important step to secure the cyber systems, but a responsive mechanism needs to be developed for monitoring and mitigating threats to systems. Hence, this paper presents the key insights about the impact of cyber terrorism and possible ICT techniques for the mitigation of threats.

Keywords: Cyber Terrorism, Cyber Crime, Cyber Security, Data Protection, Information Security.

1. Introduction

In the modern era of the internet and social media, the impact of terrorism is not limited to the local or regional level, but has become a global catastrophe. Terrorist groups and terrorist organisations are using computer technology and the internet in order to spread propaganda, commit violent acts of terror, raise funds and find new recruits. Similarly, many nation states resort to terror tactics in order to safeguard their political and national interests [1]. Terrorism involves committing acts of violence against innocent civilians and state institutions to achieve political and ideological goals. These violent acts are carried out in order to gain public attention, and pressurise governments to fulfil their demands. Thus, terrorists are a small group of bludgeon, who are willing to fight against the government with better information, advanced technology and weapons [2].

The United Nations General Secretary Report of 2004 described terrorism as - 'Any act intended to cause death or serious bodily harm to civilians or non-combatants to cause death or serious bodily harm to the civilians or non-combatants with the purpose of intimidating a population, or compelling a government, or an international organisation to do or abstain from doing any such act.' Terrorism derives its name from the word 'terrorisme'. This term was first used by the French authorities to describe the state of terror in France during the French Revolution. The word 'Terrorisme' comes from the Latin word 'terro' which means, 'I frighten'. Currently, there is no standard definition of terrorism, which is legally accepted by all nation-states. Since many countries have their own definitions of terrorism, it becomes difficult to develop a conventional narrative on terrorism [3, 4].

Similarly, terrorism has now evolved to become an international phenomenon. Countries around the world are facing multiple terrorist attacks from terror groups, who have different aims and ideology. The central theme of the terrorist is to use violence as a means to achieve political ends. It also aims to seek political attention of the masses and governments around the world. One of the key factors that contribute to the rise of terrorism lies in the exploitation of weaker sections of society over prolonged periods. Terrorism today is

used as a tool by the rogue nation-states and non-state actors in order to achieve political and ideological objectives. Junta governments along with religious organisations, cult groups, revolutionary forces, drug cartels, ruling governments, opposition parties, and pressure groups are using terrorism as a tool to commit violence [5,6].

The Indian National Security Guard Act of 1986 defines a terrorist as "Any person, who with intent to overawe the government by law establish, or with an intent to strike terror in the people or any section of the people, does any act or thing using a bomb, dynamite or other explosive substance or inflammable substances, or firearms, or other lethal weapons, or poison or various gases, or other substances (whether biological or otherwise) of a hazardous nature, in such a manner, as to cause, or as is likely to cause, death or injuries to any person or persons or damage to, or destruction of property, or disruption of any supplies or services essential to a life or community" [7-9].

2. Cyber Terrorism

Terrorism in the 21st century continues to challenge the notion of peace and stability in our modern society. Despite measures taken by the governments and law enforcement agencies, terrorism continues to echo and haunt with the emotions of fear, insecurity, and anxiety. It has taken dynamic form and mediums, which makes it difficult to contain. In the age of ICT, cyber terrorism is not restricted to the local and regional levels, but has become catastrophic in nature, and has succeeded in extending its reach globally [10-14].

This can be largely attributed to the computer and unprecedented growth of internet, coupled with the rise of new media. New media is a digital platform that provides access to digital information over the internet to web users through the medium of electronic devices and computer technology. This digital information technology includes Websites, WebPages, Web Applications, Online Radio, Live Broadcast, Live Webcast, Live TV and social media handles, which include Facebook, Twitter and Instagram, Threads and instant messaging services like WhatsApp, Viber, Snap Chat, Facebook Chat and Telegram.

Terrorists and terrorist organisations are increasingly using computer technology as a weapon to carry out terrorist activities over the internet. This has given rise to a new phenomenon called cyber terrorism. Barry Collin, a senior research fellow at the Institute of Security and Intelligence, is credited for coining the term "cyber terrorism" in 1997 [15].Collin defines cyber terrorism as the convergence of cybernetic and terrorism. Internet has not only become the backbone of the society, but more importantly, it is becoming the backbone of backbones. Internet, often called as the mother of all networks, might be better described as the lifeblood of all the networks. Today, society is more vulnerable to the attacks and failures of the internet and internet infrastructure. The merger of the online and offline life can be best described by the term "onlife". In fact, in the coming decades; the presence of online shall continue to increase. This has an important implication as to how people behave and interact online, and how this behaviour is vulnerable to cyber terrorism [16-18].With the rapid integration and advancement of internet, the nature of terrorism has acquired a new form. Modern societies of today are increasing becoming more vulnerable towards everything that is connected to the internet. These vulnerabilities are bound to be exploited by the terrorists and cyber criminals [19].
Terrorists can now hack cars and can remotely control them, and this extends to all the devices that come under the domain of internet of things. Cyber terrorism converges terrorism and cyberspace. It channelizes the systematic, unlawful attacks on computer networks and information systems, and stored data, to coerce a government or intimidate its people. Cyber terrorism today has been widely defined by various organisations and think tanks.

Cyber terrorism can be further classified into three different categories:

A. **Physical Attack:** The computer system is damaged by using conventional ways like computer vandalism, bombing, gun firing, etc.
B. **Syntactic Attack:** In this, the computer system or computer networks are wrecked by modifying the code of the system and tampering it in order to disrupt its proper functioning, and result in unpredictable irregularities. To execute this kind of attack, the attacker uses computer Viruses and Trojans.

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

C. Semantic Attack: In this attack, the perpetrator exploits the confidence of the user in the existing system, and injects tampered information in the system in order to modify and control it without the user's knowledge.

Thus, cyber terrorism today, is a modern form of terrorism. It is connected between the cyber space and terrorist activity within the realm of cyber space. There are basic methods of cyber terrorism attack: physical attack, electronic attack and attack on computer network and computer system [20, 21].

Noted expert on cyber terrorism Debra Littejohn Shinder, describes cyber-attack as an attack on computer and computer systems and networks can be defined as cyber terrorism. Such an attack can be considered an act of terror, when the effects of the destruction are destructive enough to produce fear that is comparable to the acts of physical terrorism. It is a violent form of computer crime that is committed, planned, co-ordinated in a virtual space using a computer, information technology and network.

3. Mitigation Methodology

We conducted an in-depth study to identify the key targets of cyber terrorism and followed the literature study strategy. We followed a systematic method to generate a literature database. Initially, we identified significant electronic databases for publications search with the phrase "what is cyber terrorism". The following search string is developed and applied:

(((impact of cyber terrorism *) OR (social media and cyber terrorism) OR (cyber terrorism security aspects) OR))) AND ((national security for cyber terrorism) OR (cyber terrorism *))) Based on the literature study, we developed threat mitigation strategy as shown in following Fig. 1.

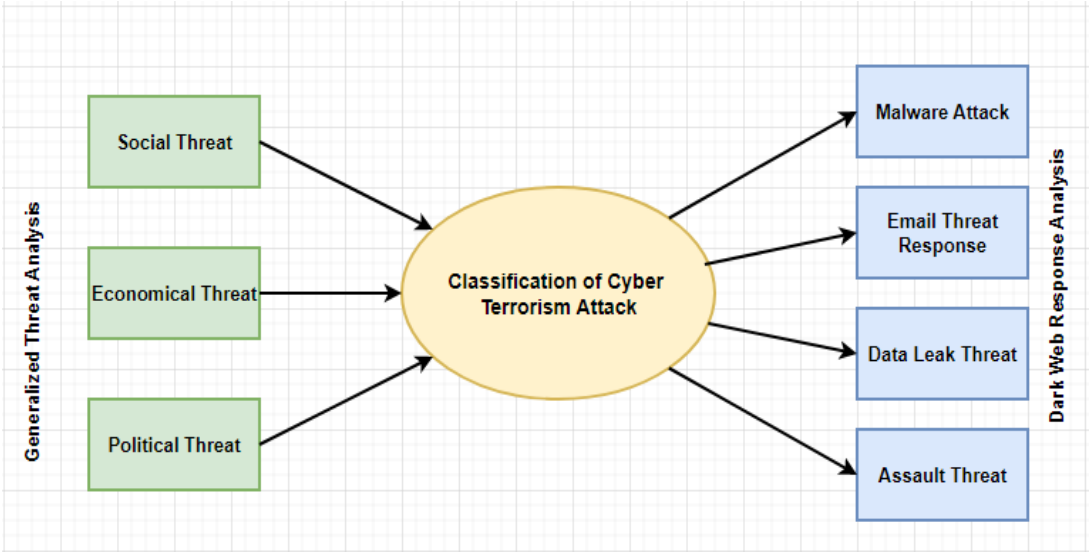

Fig.1: Proposed Cyber Mitigation Strategic Framework (Generated by the Researcher)

There is a need to classify cyber terrorism attacks and/or threat models as shown above. The mitigation strategy can be applied once the generalized threat model is transformed into specific threats. The dark web analysis system is important to identify possible attacks based on the web traffic. The segregation of web traffic can be useful to identify the type of possible attack, as shown in the above Fig.1.

3.1. Cyber Attack Analysis

According to the literature study, cyber terrorism has been evolving over the past couple of decades. The following are major cyber-attacks that left a mark in the history and context of cyber-attacks across the world. Several types of cyber-attack [22] explain the nature of threat and damage it can cause to nation-states' security and critical infrastructure.

Research Article

- 1998 - Pakistan-based hacker group Milworm, carried out web defacement attack against India's Atomic Research Center. This cyber-attack carried out by Pakistan-based organisation was one of the largest cyber-attacks against India. The hacker successfully hacked the computer system of the atomic research centre and downloaded the emails from its server. It injected messages of anti-nuclear warfare. As per an estimate, more than 100 computers were used to hack into the Indian Nuclear facility. The event received considerable international media attention. The attack was a politically motivated attack and took place at a time when India and Pakistan were under intense international pressure to accept and acknowledge the presence of nuclear weapons.
- 2007 - Denial of Service attack on the Estonian government cyber networks following disputes with Russia over the removal of Russian War Memorial. This cyber-attack succeeded in crippling the essential services of Estonia and took several days for the Estonian officials to restore its cyber system and bring it back online.
- 2007 - Unclassified email account of the US Secretary of Defence was hacked. This attack was carried out to exploit sensitive information from the Pentagon computer systems and network. This attack resulted into serious breach of national security using cyber space and computer.
- 2009 - Israel's critical infrastructure placed under attack. The attack took place on Israel's Internet Infrastructure. Hamas and Hezbollah were responsible for the attack. This attack was carried out on government systems and websites and successfully infected more than five million computers.
- 2010 - Iran's Cyber Army disrupts China's search engine Baidu. The users were re- directed to a web page that displayed an Iranian political message.
- 2014 - Russia based hackers took down Ukraine's Election Commission System. This cyber attack took place few days before the Ukrainian Presidential Election. The attack was carried out to benefit Pro–Russian candidates and cause damages to the Ukrainian Candidates.
- 2015 - Cybercriminals attack computer systems of the German Parliament, causing widespread disruption and panic. It is estimated that more than 20,000 computers used by the German politicians and authorities of the parliament were subjected to attack. The attackers had made a Ransome demand, amounting to millions of euros to clean up the damages.
- 2016 - Russian coordinated cyber-attack on Ukraine's critical infrastructure. The attack was carried out on Ukraine's Electric Grid System. More than 225,000 customers had to face power blackout due the failure of the Electric Grid System. A denial of service of attack along with malware attack was carried out.
- 2016 - The United States Department of Justice convicts Ardit Ferizi and sentences him to 20 years of imprisonment for providing sensitive information to the terrorist organisation, Islamic State of Iraq and the Levant. Ardit Ferizi gained access to protected computers without any proper clearance or authorization. This illegal access was used to obtain sensitive material, which was later provided to ISIL organisation.
- 2017 - Hackers associated with the North Korean government carried out a massive cyber-attack against Sony Corporation. The attacker had warned Sony Corporation of an imminent cyber-attack if Sony Pictures release the movie 'The Interview'. This movie defames North Korean Regime and its leader Kim Jong Un. Despite threats been issued, the movie was scheduled for release in the USA. Days after its initial release, a massive cyber-attack took place on Sony Corporation, which forced Sony Pictures to withdraw its screening of the movie.
- 2017 - Wanna Cry virus executed worldwide. This virus had affected major corporations, companies, government offices and hospitals around the world. WannaCry virus was a Ransomware attack, which affected more than 75,000 computers in 99 countries of the world, as estimated by Avast, a cyber-security firm. Cyber experts believe that North Korea, particularly the Lasarus Group, was responsible for the attack and release of the WannaCry virus globally.
- 2021 - Ransomware attack took place on Colonial Pipeline causing disruptions in supply chain network leading to fuel shortages and oil price rises in the United States.
- 2022 - Chinese affiliated cyber actors carried out cyber attacks against small island nations of Southeast Asia for cyber espionage.

4. Key Targets of Cyber Terrorism

According to the literature study analysis we identified following key targets of Cyber Terrorism:

1. Attack on Power Grids – Sabotage industrial control systems of power grid that control power distribution networks resulting into loss of power and loss of electricity. Such attacks on power grids can cause

Research Article

repeated power failure, which might take several days or weeks to restore power distribution system and its supply network. Denied access to stable electricity for longer periods can cripple facilities like Online Banking, ATM Machines, Metro Rail, Disrupt Supply Chains, Blackouts, Etc.
2. Attack on Health Care System - Sabotage database of hospitals by deleting patient's databases and deny access to prescribed methods of treatment to critical patients who have life-threatening diseases.
3. Attack on Water Distribution System - Sabotage Water Purification Systems and mix sewage water with drink water system, polluting drinking water system, resulting in spreading of life-threatening diseases
4. Attack on Air Traffic Control System - Sabotage command-and-control system (air traffic control system) for air traffic, resulting in panic and crashing of commercial aircraft.
5. Attack on Transportation System - Sabotage Traffic Control System, causing widespread panic on streets, traffic snarls, long queues of vehicles and even deaths resulting due to accidents caused by absence of proper signal management.

5. Conclusions

As the mitigation model framework is discussed in this paper, it is proven that social media has made an unprecedented impact on societies across the world. It is increasingly being used for extending human networks beyond the conventional boundaries and connecting with new people. It has technological capability and public outreach to convey a considerable amount of information into the public domain and impact a significant number of populations across the globe. Social media tools like voice calls, live chat sessions, blogs, WebPages, and technologies like Facebook, Twitter, Telegram, TikTok, Reddit, Zoom are popular among its users. On the other hand, some ill-minded groups are using it to spread social tensions. Terrorists often use social media technology and the internet as crucial tools to achieve organisational goals and objectives. Internet technology and social media tools have proven to be an effective mode of recruiting and radicalising youths and making them part of its organisation. The increasing radicalization through social media has turned several susceptible youths towards extremism.

References:

[1]Smith, Katherine Taken, et al. "Cyber terrorism cases and stock market valuation effects." Information & Computer Security 31.4 (2023): 385-403.
[2]Broeders, Dennis, Fabio Cristiano, and Daan Weggemans. "Too close for comfort: cyber terrorism and information security across national policies and international diplomacy." Studies in conflict & terrorism 46.12 (2023): 2426-2453.
[3]Naidoo, Rennie, and Carla Jacobs. "Cyber warfare and cyber terrorism threats targeting critical infrastructure: a hcps-based threat modelling intelligence framework." ECCWS 2023 22nd European Conference on Cyber Warfare and Security. No. 1. Academic Conferences and publishing limited, 2023.
[4]Chawla, Ajay. "Cyber-Terrorism A Wicked Problem." Journal of Criminology and Forensic Studies 5.1 (2023): 180058.
[5]Melnyk, D. S. "Cyberterrorism: content, forms and promising countermeasures." Bull. Kharkiv Nat'l. Univ. Internal Aff. (2023): 144.
[6]Bernatzky, Colin, Matthew Costello, and James Hawdon. "Who produces online hate?: An examination of the effects of self-control, social structure, & social learning." American journal of criminal justice 47.3 (2022): 421-440.
[7]Li, Carrie KW. "The applicability of social structure and social learning theory to explain intimate partner violence perpetration across national contexts." Journal of interpersonal violence 37.23-24 (2022): NP22475-NP22500.
[8]Golose, Petrus Reinhard. "A comparative analysis of the factors predicting fears of terrorism and cyberterrorism in a developing nation context." Journal of Ethnic and Cultural Studies 9.4 (2022): 106-119.
[9]Shandler, Ryan, et al. "Cyber terrorism and public support for retaliation–a multi-country survey experiment." British Journal of Political Science 52.2 (2022): 850-868.
[10]Golose, Petrus Reinhard. "Cyber Terrorism-A Perspective of Policy Analysis." International Journal of Cyber Criminology 16.2 (2022): 149-161.
[11]Dearden, Thomas E., and Katalin Parti. "Cybercrime, differential association, and self-control: Knowledge transmission through online social learning." American Journal of Criminal Justice 46.6 (2021): 935-955.

[12]Costello, Matthew, Salvatore J. Restifo, and James Hawdon. "Viewing anti-immigrant hate online: An application of routine activity and Social Structure-Social Learning Theory." Computers in Human Behavior 124 (2021): 106927.
[13]Plotnek, Jordan J., and Jill Slay. "Cyber terrorism: A homogenized taxonomy and definition." Computers & Security 102 (2021): 102145.
[14]Lee, Claire Seungeun, et al. "Mapping global cyberterror networks: an empirical study of al-Qaeda and ISIS cyberterrorism events." Journal of Contemporary Criminal Justice 37.3 (2021): 333-355.
[15]Wolfowicz, Michael, et al. "Faces of radicalism: Differentiating between violent and non-violent radicals by their social media profiles." Computers in Human Behavior 116 (2021): 106646.
[16]Bossler, Adam M. "Neutralizing cyber attacks: Techniques of neutralization and willingness to commit cyber attacks." American Journal of Criminal Justice 46.6 (2021): 911-934.
[17]Nodeland, Brooke, and Robert Morris. "A test of social learning theory and self-control on cyber offending." Deviant Behavior 41.1 (2020): 41-56.
[18]Hawdon, James, and Matthew Costello. "Learning to hate: Explaining participation in online extremism." Radicalization and Counter-Radicalization. Emerald Publishing Limited, 2020. 167-182.
[19]Shapiro, Lauren R., and Marie-Helen Maras. "Women's radicalization to religious terrorism: An examination of ISIS cases in the United States." Islamic State's Online Activity and Responses. Routledge, 2020. 88-119.
[20]Nnam, Macpherson Uchenna, et al. "The War must be Sustained: An Integrated Theoretical Perspective of the Cyberspace-Boko Haram Terrorism Nexus in Nigeria." International Journal of Cyber Criminology 13.2 (2019).
[21]Marsili, Marco. "The war on cyberterrorism." Democracy and security 15.2 (2019): 172-199.
[22]Yaokumah, Winfred. "Cyber security competency model based on learning theories and learning continuum hierarchy." Global cyber security labor shortage and international business risk. IGI Global Scientific Publishing, 2019. 94-110.