Content available at: https://www.ipinnovative.com/open-access-journals

IP International Journal of Forensic Medicine and Toxicological Sciences

Journal homepage: http://www.ijfmts.com/

Review Article

A comprehensive review study of cyber terrorism and novel developments in the current scenario

Anuwanshi Sharma[1]*

[1] *Dept. of Forensic Science, Galgotias University, Greater Noida, Uttar Pradesh, India*

ARTICLE INFO

Article history:
Received 08-10-2023
Accepted 25-11-2023
Available online 19-01-2024

Keywords:
Internet safety
New trends key administration
Information techniques
Cyberattacks

ABSTRACT

The widely held of global trade and industry, profitable, traditional, communal, and administrative connections and actions—those of people, governments, and political organizations—now take place accessible. In recent years, cyber-attacks and the dangers of wireless message tools have become challenges for numerous viable enterprises and constitutional organizations all over the world. In contemporary culture, electronic technology is widely employed. Therefore, safeguarding sensitive data from cyber-attacks is a challenging task. Cyber-attacks may also be employed to further military or political objectives. These are a few effects of data distribution services (DDS), computer viruses, knowledge gaps, and other attack vectors. Numerous businesses have a variety of defenses against cyber-attacks. In real time, cyber security keeps up with the most recent information technology developments. Researchers from all around the world have put forth several strategies up until recently to inhibit cyber-attacks or diminution the destruction they reason. Although certain systems are presently in custom, others are quiet being investigated. The objective of this study is to analyses and carefully analyses the regular developments prepared in the zone of cyber safety as well as appearance into the challenges, benefits, and detriments of the proposed solutions. Furthermore, recent advances in cyber security, security problems, and threats are explored.

1. Introduction

For more than two eras, the Internet has played a significant part in worldwide communication; becoming progressively incorporated in individual's every day exists. The Internet presently has around 3 billion users worldwide as a result of breakthroughs and low-cost expenses in this industry that have suggestively improved its accessibility, use, and act.[1] Because the Internet has formed a large international network, the worldwide budget now produces billions of dollars per year.[2] The bulk of international financial, commercial, national, social, and administrative connections and actions now take place online, according to Aghajani and Ghadimi. Interactions between people, non-governmental organizations, governments, and governmental institutions are all included. Most vigorous and delicate data is conveyed to or designed in this space, as vital and sensitive infrastructures and systems are either a part of cyberspace or are controlled, managed, and exploited through it.[3] The bulk of financial transactions take place in this area, as do the majority of media activities, and a significant portion of individuals' time and activities are spent interacting in this space. The contribution of money from internet enterprises to a nation's Gross Domestic Product (GDP) has expanded considerably, and accessible measures make for a sizable share of the metrics used to assess the level of growth.

A major amount of a nation's substantial and divine capital is invested in this sector, as is a corresponding

* *Corresponding author*.
E-mail address: anuwanshisharma@gmail.com (A. Sharma).

https://doi.org/10.18231/j.ijfmts.2023.029
2581-9844/© 2023 Author(s), Published by Innovative Publication.

portion of a citizen's personal riches and spiritual accomplishments. In other words, many features of residents' lives are intricately tied to one place, and any disturbance, uneasiness, or struggle there will have a direct effect on other characteristics of individual's lifecycle.[4] Managements, on the other hand, are now confronted with new security challenges as a result of cyberspace. The low entry barrier, anonymity, unpredictability of the threatening geographical area, dramatic impact, and lack of public transparency in cyberspace have given rise to threats such as cyber warfare, cybercrime, cyber terrorism, and cyber espionage among strong and weak actors such as governments, organized crime groups, and even individuals.[5]

2. Definition of a Cyber-Attack from the Perspective of Experts

The following are the most significant explanations of a cyber-attack that have been provided by experts in the legitimate and technological fields:

According to Motsch et al. (2020), cyber-attacks are activities conducted by states to breach the systems or processor systems of a state or other states to interrupt or create destruction. In the study and criticism of this explanation, it may be claimed that the three criteria—the attacker, the attack's goal, and its purpose—have been applied without taking disruption types into account. Additionally, only countries are mentioned in terms of the attacker in overall; though, if an attack occurs in a perspective or topographical zone that is below the regulator and authority of a nation (such as a network controlled by a country in cyberspace), it will essentially decrease external the definition declared and exclude non-governmental and remote clusters, and as a result, there should be a gap. Given the circumstances, it may be argued that the aforementioned definition is essentially inadequate; left out a major quota of assaults carried out by commercial and non-governmental administrations, and creates a gap.

According to Michael Hayden: some deliberate effort to damage or interfere with the computer networks of another nation. This term is quite broad and does not distinguish between cybercrime, cyber-attacks, and cyber warfare; as a result, the boundary between their discoveries is murky. The absence of such a boundary will undoubtedly have an impact on commentators' and policymakers' decisions. The general context of the laws of warfare leaves the internet unregulated, which may undoubtedly have harmful and detrimental effects on the development of war and nation-state belligerence.[6] Because of this, the preceding definition's fundamental flaw—which results in a lack of luck—is its universality. In contrast to the major description, which restricted the attack's offenders to administration attackers, this description is broad and simple to understand, which makes it potentially dangerous and dangerous for international peace.[7] It can also have unfavorable effects and confuse international relations.

Martin Libicki: Computer systems that have been subjected to digital assaults appear to be operating normally but create and issue false replies. This definition of a cyber-attack leaves out a broad variety of possible risks to the nationwide safety of a nation whose cyber infrastructure has been attacked but has not yet touched the intensity and threshold of significant assaults. The target nation's computer systems and networks are susceptible to damage from these threats. Any explanation of a cyber-attack that does not include the aforementioned would thus be insufficient and lack the requisite all-inclusiveness.[7]

Tallinn Manual Group: It is aggressive or self-protective cyber activities that have the prospective to destruction or destroy individuals harm goods or both. The findings and impacts obtained are actually what make this definition ambiguous. If a cyber-attack results in the outcomes specified in the description (i.e., the infliction of individual and economic harm), then, in the opinion of the definition's authors, it is an attack. As a result, if this kind of attack leaves behind objective and perceptible belongings and penalties of violence, it will be classified as an attack, and it is at this point that the guidelines of international rule in associated areas (the right to invoke compulsion, the law of war, and the law of international accountability will be enforced) will come into play.

3. Approaches to Cyber Terrorism

Cyber terrorist organizations want to reason extensive chaos, interrupt serious substructure, stimulate political action or hacktivism, and even grounds bodily wound and even fatalities. Cyber terrorists use a range of methods. Among them are the following assault types:

1. Advanced persistent threats (APTs) are attacks that use complicated and targeted network infiltration techniques. The attackers seek to take data while remaining undetected within the network. APT attacks usually target organizations with sensitive information, such as those in countrywide defense, industrialized, and finance.
2. Malware, computer worms, and viruses are precisely designed to attack IT control methods. They are used to launch attacks against military organizations, conveyance systems, electrical networks, and serious substructure.
3. DoS attacks attempt to prevent authorized operators from retrieving specified computer organizations, strategies, or computer systems. These cybercriminals commonly target administrations and critical substructure. The purpose of hacking, or gaining unauthorized admittance, is to steal vital information from organizations, administrations, and marketable

entities.

4. Ransom ware, a virus, grasps facts systems captive until the victim pays the demanded money. Furthermore, some ransom ware attacks exfiltrate data.
5. Phishing efforts to collect information from a target's electronic message and then use that information to obtain admittance to methods or take the victim's personality.

3.1. What are some instances of online terrorism?

Cyber terrorists use computer servers, other strategies, and systems manageable via the public internet. Protected administration systems and other controlled systems are routinely targeted. Instances of cyber terrorism contain the following:

1. Large websites are being disrupted. In this condition, the purpose is to irritate the general community or to avoid admittance to websites that comprise material that the hackers discover offensive.
2. Unauthorized access- Attackers routinely try to interrupt or change communications that control military tools or other critical equipment.
3. Critical substructure organizations are being jeopardized. Risk actors try to paralyses or interrupt capitals, create a community wellbeing emergency, jeopardize public safety, or instill a lethal panic. A water treatment facility, an oil factory, a pipeline, or fracking activities might all be aims of cyber terrorists.
4. Cyber espionage- Administrations commonly participate in or encourage cyber espionage. They want to spy on rival nations and learn about military actions and conflict tactics.[8]

4. Cyber Terrorism 26/11 Incident

London Attack On November 26, 2008, Bombay was the scene of an appalling episode that lasted four days and involved 12 match firings and bombings. Undoubtedly, this was a significant cyber-attack against the nation. The fear cluster terrorist gang, which consisted of ten Pakistani men, assaulted buildings in Bombay, murdering 164 people. Nine markswomen were also murdered during the assaults, although one escaped. They started their journey by boat from Karachi, West Pakistan, to Bombay. They took control of a fishing boat, murdered four crew members, and slashed the captain's throat.[9] Terrorists thrived in the area of the Bombay megacity near to the Republic of India monument. They used explosives and automatic firearms to take control buses and police cars. Terrorists used brightly coloured computers and telephones to enter the systems of the Taj Hotel, Leopold Cafe, Shivaji Maharaj Terminal, Oberoi Trident, giving them access to all of the hostel's data as well as those of other sites. Its intended victims were foreign visitors from countries like the U.S., the U.K., and others. The explosions persisted for four days. One of the significant events in our nation was November 26, which made the government concerned about cyber security and cybercrime.

5. The WannaCry Outbreak Incident

With the development of computer security techniques, worm breakouts have become increasingly rare since it is challenging to obtain malware that will operate autonomously on a remote machine without the involvement of a stoner. The WannaCry was a worm in the language of computers. It was a particular kind of malware that had the potential to spread widely and become far more harmful than a typical computer infection. This type of worm tone replicates, bouncing from host to host and conforming to all the regulations. When it infects well-connected bumps through the Garcon Communication Block protocol, it grows significantly and takes off. In April 2017, a shadowy hacker organization known as The Shadow Breakers discovered a flaw in Microsoft's Windows operating system that could be exploited to launch apps automatically on other machines connected to the same network. The outbreak did indeed cause significant harm when the kill switch was used. The worm translated lines on the computer's hard disc after infecting Windows machines, making it impossible for drug users to penetrate the drive.

The spyware required a bit coin rescue payment and the loss of access to interpreting them; otherwise, the lines would have been permanently wiped. Almost 80 NHS organizations in England had their computers shut down owing to the WannaCry epidemic, which led to the cancellation of 20,000 moving parts and the diverting of ambulances that were not equipped to manage emergencies. The virus caused problems with life, health, and significant cash. This cybercrime is thought to have cost businesses around the world $4 billion in damages. Instead of alerting the InfoSec community, it was believed that the U.S. National Security Assistance identified this vulnerability and mishandled the knowledge by creating legislation to exploit it, dubbed Eternal Blue.[10] Microsoft published SMB updates two months before the incident, yet the epidemic exposed and severely harmed patch less Computers. The business stated that the equipment only suffered minor damage. Due to the publicity surrounding the assault and the easily accessible Microsoft fixes, Boeing was able to cease the attack and resume operations. In a couple of hours, WannaCry infected hundreds of thousands of machines across more than 150 countries. It spread like wildfire. It was a first for the world that a virus could propagate over the planet and encrypts a stoner's lines while requiring bit coin to open them. This had serious consequences for the NHS and its ability to care patients. These consequences may have been avoided if the NHS had agreed to follow fundamental information technology security rules that had been made public and prescribed.[11] To ensure that what happened in the NHS case is better protected against future attacks, the entire globe must band together.

6. The Psychosomatic Impact of Cyber Terrorism

The findings show that cyber terrorism, even when non-lethal, has an impact on the broader public in a variety of ways. Second, cyber terrorism increases people's anxiety and unease about themselves. Second, both fatal and non-lethal acts of terrorism heighten feelings of fear and anxiety. Finally, many people, particularly those who regard dangers as serious, are likely to support severe government controls. These strategies are classified into two sorts: international procedure (for example, kinetic or cyber-based martial replies to cyber-attacks) and local policy (for instance, acceptance of administration investigation and Internet control). People embrace more conservative political positions as their sense of threat grows. Cyber terrorism, like customary terrorism, toughens radical beliefs because individuals are eager to give up their municipal authorizations and confidentiality for defense. They also favor increased management monitoring, tighter Internet regulations, and aggressive martial replies to cyber-attacks. The public speech required for a dynamic and exposed autonomous civilization may be negatively impacted by these restrictions, even though they are intended to guarantee national security.[12]

But, unlike traditional terrorism, cyber terrorism does not seriously erode public trust in the state management or its associations. The confidence processes contrasting a control cluster to those visible to conventional and cyber-terrorism representations made this conclusion clear. As stated at the beginning of this essay, terrorism or other traumatic events may not always impact such broad measures of confidence. On the contrary, as happened in the USA after 9/11, such incidents frequently increased popular trust. These confidence-related findings are in line with calls for increased security. People cannot show a lack of faith in the government without feeling uneasy because they desire more government control, especially those with great stages of danger insight. Advocates of extensive administration control and monitoring must believe that the authorities will carry out their duties competently and ethically, given their increased power.

This does not imply that governments can do nothing. In addition to managements in the USA, Europe, and other countries, this is true for Israel's governments, whose people were the focus of this exploration. The impacts of cyber terrorism in Israel are similarly significant, much as studies of the psychology of terrorism in Israel from the 20th century influenced post-9/11 studies. Cyber terrorism is a global spectacle, and we can see that groups like unspecified are similarly prepared to damage Israeli systems as American ones (as in Ferguson, Missouri, in 2014). In reality, as study advances, the repercussions of cyber terrorism may be less severe in Israel than elsewhere. Hamas is a well-known entity to Israelis, a partner in a protracted but, so far, controllable war that periodically explodes into persistent bloodshed. Hamas must make its demands and assaults known to achieve its objectives. That is not a problem to attribute.

On the other hand, this is not always the case for ISIS and the agents of unfriendly countries. Attacks are tough to feature, and hacktivist demands are frequently unidentified, making it possible for foreign governments to use proxies to carry out hostile cyber operations. Such assaults prey on unpredictability and disruption, which might worsen nervousness, threat perception, and threat insight in more Western states than we have observed in Israel.

The disproportionate risk attributable to threats to life, limb, and infrastructure is consistent with earlier research that found that hazards associated with uncertainty and dread risk, or events "perceived by lack of control, dread, catastrophic potential, and fatal consequences," were associated with relatively high levels of risk perception. According to Lichtenstein et al., exposure to the media, especially sensationalized media coverage, catastrophic results, and a lack of first-hand experience might bias risk evaluations. Cyber terrorism somewhat matches these paradigms. Although there are only speculative links between cyber-attacks and mass casualties, the high risk associated with infrastructure damage and loss of life and limb may be explained by their potentially catastrophic effects, the advantages they offer (making them a likely target as well as a significant source of concern if threatened), the inability to always identify perpetrators or their motivations, and expert disagreements that only exaggerate.[13] Although the impact of media coverage has yet to be thoroughly investigated, it may shed light on the substantial hazards that many people identify with cyber terrorism. Slovic also reminds us that kinetic terrorist attacks have high "signal value," or the idea that an incident will have a lasting impact and result in further devastation, death, and chaos. As a result, the danger is overestimated. According to the research, however, cyber terrorism has never resulted in fatalities or injuries. Cyber risk is therefore expected to be the next frontier of risk perception theory due to its distinctive counterfactual.

7. Russian–Ukrainian Cyber Warfare

Since the demise of the Soviet Union in 1991, cyber warfare has played a part in Russia-Ukraine conflict. Uroburos, a Russian cyber weapon, has been circulating since 2005. However, the first attacks on commercial company and government computer systems in Ukraine were observed during large-scale protests in 2013. Russian cyber warfare resumed in December 2016, with the paralysis of the Ukrainian State Treasury, a huge hacker supply-chain assault in June 2017, attacks on Ukrainian government websites in January 2022, and hacks into Ukraine's power system in 2015 and 2016. Russian cyber-attacks on Ukraine have been continuous since Moscow's unlawful takeover of Crimea in 2014, reaching a climax proximately previously the 2022 assault. Russia launched war on Ukraine on February 24, 2022. During this period, Ukraine's community, vitality, media, monetary, profitable, and nonprofit areas have suffered the most. Meanwhile February 24, incomplete cyber-attacks by Russia have impeded the supply of nutrition, medicine, and humanitarian aid. Its consequences have included data theft and deceit, particularly with deep fake technologies, as well as restrictions on access to critical services.

Other risky online behavior includes phishing electronic mail, dispersed denial-of-service assaults, facts-wiper malware, stage door, investigation software, and statistics thieves. Organizations and managements all across the world have taken notice of the hybrid risks offered. Enterprises directed by the EU, the US, and NATO have been implemented to combat cyber extortions and protect key substructure. As measure of these operations, the EU has established Cyber Rapid Reaction Teams, an initiative under PESCO (Permanent Structured Cooperation) in safety and defense strategy. Through numerous cyber-resilience efforts, Ukraine has received aid from non-governmental and private organizations. Unaffiliated hackers have launched many counterattacks on the Russian government, security, banking, and media networks since the invasion began. According to the European Parliament, the EU's cyber-sanctions regimes should be employed to the utmost degree possible against individuals guilty for or complicit in the multiple cyber-attacks on Ukraine.[14]

8. Cyber Incidents in the UK

Businesses and organizations in the UK reported hundreds of cyber events to the NCSC over the course of the last year, 63 of which were serious enough to call for a national-level response. A variety of harmful cyber activities, including ransom ware, reconnaissance, malware, network intrusions, data exfiltration, and interruption of services and systems, were involved in the events. The NCSC worked all year with its partners, including the NCA, to develop a whole system approach, respond to incidents as they happened, and assist victims in recovering while trying to prevent as many attacks as possible from getting through (2.1 million commodity campaigns were removed). The commercial cyber incident response market has developed more during the past year. It is becoming increasingly typical for cyber insurance plans to include comprehensive support packages that include technical support from cyber incident response organizations as well as legal aid. Companies dealing with sophisticated, targeted assaults against networks of national significance are guaranteed by the NCSC's Cyber Incident Response (CIR) Level 1 plan. The NCSC intends to expand this in the upcoming year to include a Level 2 program that will offer technical responses for events impacting small to medium-sized businesses that need more approachable CIR help. Following several high-profile incidents, such as the attack on the Colonial Pipeline in the US, ransom ware disrupted critical national infrastructure organizations last year.[14] However, public outcry and increased political interest have raised the stakes for cybercriminals. It soon became apparent that certain organizations had altered their tactics in response to evading the use of force, sanctions, and other operational measures.

9. Future Threat Controversies

According to the NCSC, the propagation and commercial accessibility of cyber competences will raise the UK's cyber safety risk in the upcoming years. Future state and non-state actors will have access to additional harmful and disorderly cyber technology, which will be utilized more commonly and unpredictable. These vast and complex ecosystems includes the accessibility of off-the-shelf cyber-surveillance tools and connected facilities, the vulnerability and exploit shop, hackers-for-hire offering specialized hacking facilities, and the deployment of malware that is whichever widely or commercially exist. The growing black market for cyber tools drops the access hurdle for governments, making it easier for them to get capability—some of which will be highly sophisticated and advanced—and, as a result, intelligence that they may not otherwise develop or acquire. Because of the significant demand for these goods and services, we believe that the sector will continue to grow. Non-state actors' entry barriers are also being lessened through hacker-for-hire and "as-a-Service" models. Ransom ware as a Service (RaaS) is one instance of how this abundance enables fewer skilled criminal performers to extract administrations. In a speech delivered during Tel Aviv Cyber Week in June 2022, Lindy Cameron emphasized the difficulty that the proliferation of cyber capabilities poses. She said: "If we are going to sustain a cyberspace that is a not dangerous and flourishing residence for everybody, it is vigorous that such competences are created and used in a mode that is permitted, accountable, and balanced.

10. Discussion

In the third millennium, one of the most significant power sources is the internet and related technologies. Power dissipation is a phenomenon brought about by the characteristics of cyberspace, including low entry costs, anonymity, vulnerability, and asymmetry. This means that if governments have so far divided the power struggle among themselves, then other actors—such as individuals, private enterprises, and organized criminal and terrorist groups—must be involved, though governments continue to play a significant role. Governments will not lose their national security as a result of this phenomenon. Numerous methods can be used to assess this impact. Today, the possibility of people's quality of life falling is a challenge to national security; it is no longer possible to define national security in terms of military concerns and internal and external boundaries. Governments are not the only entities that face cyber risks; people and businesses can also suffer from these dangers.

11. Conclusion

India and the rest of the world are also seeing exponential growth in cybercrime. Intellectual property theft, cyber terrorism, cyber extortion, and sexual harassment are just a few of the crimes committed in cyberspace that have been in-depth examined in this article, along with the relevant legislation in the context of Indian law. Also, the study presented a comparison of the Budapest Convention and Interpol's response to the rise in cybercrime. Legal professionals from across the world and in India will need to be adept at working with various information sources, developing novel ways to query them, and using the information to give their clients timely and proactive guidance. The requirement for security in electronic networks creates new difficulties. As chances for growth exist in the information era for those who can best use both technology and information, it is time for the Indian legal system to keep up with the expanding cybercrimes and the evolving international jurisprudence surrounding them. The necessity for this transformation has grown more pressing and essential with the migration of information to the cyber sphere in the wake of the COVID-19 epidemic. To secure India's cyberspace, statutory laws, government policies, and specialized investigative agencies would be beneficial. Through legal awareness programs, the public should be given the knowledge necessary to protect themselves against the hazards posed by cybercrime. India's digital future rests on a fulcrum, and the moment has come to move that fulcrum toward safety and security about cybercrimes.

12. Source of Funding

None.

13. Conflict of Interest

None.

References

1. Aghajani G, Ghadimi N. Multi-objective energy management in a micro-grid. *Energy Rep*. 2018;4:218–25.
2. Jamal AA, Majid AAM, Konev A, Kosachenko T, Shelupanov A. A review on security analysis of cyber physical systems using Machine learning. *Materials Today: Proc*. 2023;80(3):2302–6.
3. Hejazi HA, Mohsenian-Rad H. Power systems big data analytics: An assessment of paradigm shift barriers and prospects. *Energy Rep*. 2018;4:91–100.
4. Amir M, Givargis T. Pareto optimal design space exploration of cyber-physical systems. *Internet of Things*. 2020;12:100308.
5. Bullock JA, Haddow GD, Coppola DP. Cyber security and critical infrastructure protection. In: and others, editor. Introduction to Homeland Security; 2021. p. 425–97.
6. Cao Y, Huang Z, Ke C, Xie J, Wang J. A topology-aware access control model for collaborative cyber-physical spaces: Specification and verification. *Computers & security*. 2019;87:101478.
7. Judge MA, Manzoor A, Maple C, Rodrigues JJ, Islam S. Price-based demand response for household load management with interval uncertainty. *Energy Rep*. 2021;7:8493–504.
8. Li J, Sun C, Su Q. Analysis of cascading failures of power cyber-physical systems considering false data injection attacks. *Glob Energy Interconnection*. 2021;4(2):204–13.
9. Nguyen L, Golman C. Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries:'Law on the books' vs 'law in action. *Comp Law Secur Rev*. 2021;40:105521.
10. Niraja KS, Rao SS. WITHDRAWN: A hybrid algorithm design for near real time detection cyber-attacks from compromised devices to enhance IoT security; 2021. Available from: https://shorturl.at/sD359.
11. Priyadarshini I, Kumar R, Sharma R, Singh PK, Satapathy SC. Identifying cyber insecurities in trustworthy space and energy sector for smart grids. *Comp Electr Eng*. 2021;93:107204.
12. Quigley K, Burns C, Stallard K. Cyber Gurus': A rhetorical analysis of the language of cybersecurity specialists and the implications for security policy and critical infrastructure protection. *Govt Inf Q*. 2015;32(2):108–17.
13. Shamel A, Marefati M, Alayi R, Gholaminia B, Rohl H. Designing a PID controller to control a fuel cell voltage using the imperialist competitive algorithm. *Adv Sci Technol Res J*. 2016;10(30):176–81.
14. Tan S, Xie P, Guerrero JM, Vasquez JC, Li Y, Guo X. Attack detection design for dc micro grid using eigenvalue assignment approach. *Energy Rep*. 2021;7(1):469–76.

Author biography

Anuwanshi Sharma, Research Scholar https://orcid.org/0000-0002-6841-8564

Cite this article: Sharma A. A comprehensive review study of cyber terrorism and novel developments in the current scenario. *IP Int J Forensic Med Toxicol Sci* 2023;8(4):132-137.