IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

# Cyber Warfare And Cyber Terrorism: A Review

[1]Ayush Singh [2]Mohit Raval [3]Dr. Monika Patel
[1,2]Student [3]Asistant Professor
[1,2]S.V Institute of Computer Studies, Gandhinagar, India.
[3]S K Patel Institute of Computer Studies, Gandhinagar, India.

***Abstract:*** Cyberspace has a hidden, dangerous side where cyber warfare and cyber terrorism pose major threats. Cyber warfare involves digital attacks by nation-states to disrupt another country's infrastructure, military, or government systems, often for strategic or political gains. These attacks include malware, phishing, and denial-of-service (DoS) attacks. In contrast, cyber terrorism is conducted by non-state actors, aiming to create fear and chaos by targeting civilians, essential services, and financial institutions through techniques like website defacement, ransomware, and cyber talking. Both cyber warfare and cyber terrorism exploit system vulnerabilities and are difficult to defend against due to their anonymous and borderless nature. The rising number of cyber incidents highlights the need for strong cybersecurity measures, global cooperation, and advanced defense strategies. This paper explores the key differences, types, and impacts of cyber threats while emphasizing the importance of continuous research and technological advancements to combat them. Strengthening cybersecurity is crucial to maintaining national security and public safety in an increasingly digital world.

**Index Terms** – Cyber Warfare, Cyber Terrorism, Malware, Phishing, Cyber Security, Digital Attacks, Cyber Crime

## 1. INTRODUCTION:

This review aims to help readers easily distinguish between cyber warfare and cyber terrorism.

In today's digital age, the threats of cyber terrorism and cyber warfare have become significant concerns for nations and organizations worldwide. Cyber terrorism refers to the use of the internet and digital tools by terrorist groups to conduct attacks. These attacks aim to cause harm, fear, and disruption. For example, terrorists might hack into critical infrastructure like power grids or financial systems, leading to chaos and potentially endangering lives.

Cyber warfare, on the other hand, involves state-sponsored attacks. Countries use cyber techniques to spy on or damage the digital assets of rival nations. These attacks can target government networks, military systems, or key industries, aiming to weaken an opponent without traditional military conflict. Examples include the use of malware to disrupt a country's nuclear program or to steal sensitive defense information.

Both cyber terrorism and cyber warfare exploit vulnerabilities in computer systems and networks. They can be difficult to defend against because attackers can operate from anywhere in the world, often anonymously. The impacts of these attacks can be extensive, affecting not only the immediate targets but also causing widespread economic and social disruption.

The rise of these cyber threats has led to increased efforts in cybersecurity. Governments and organizations are investing in advanced technologies and strategies to detect, prevent, and respond to cyber attacks. International cooperation is also crucial, as cyber threats often cross borders.

Understanding and mitigating the risks associated with cyber terrorism and cyber warfare are critical for maintaining national security and public safety in our increasingly interconnected world. This review paper will explore the nature, impact, and defense strategies related to these emerging threats, highlighting the importance of robust cybersecurity measures in protecting against digital attacks

## 2. DEFINITION OF CYBER WARFARE:

In (GOOD, 2015) define cyber warfare as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption," encompassing a wide array of activities such as attacks on critical infrastructure, military systems, and civilian targets to achieve strategic, military, or political objectives.

Similarly, in (Robinson et al., 2015) describe cyber warfare as the use of digital assaults by one country to interfere with the operations of another, focusing on attacking information systems, essential infrastructure, and communication networks. Combining these definitions, cyber warfare can be understood as the strategic use of digital attacks by nation-states to disrupt the operations of another nation by targeting their computers, networks, critical infrastructure, military systems, and communication networks to achieve political, military, or strategic goals (GOOD, 2015), (Robinson et al., 2015).

### 2.1 TYPES OF CYBER WARFARE:

**1) Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks**

**DoS**: Denial of services means make server busy with traffic and Overload so a system or server with requests to make it unavailable to users (Elleithy & Blagovic, 2006).

**DDoS:** Distributed Denial of Service means it is a cybercrime in which attacker floods a server with traffic to prevent user from accessing online services and sites (Elleithy & Blagovic, 2006). DDoS attack is DoS attack that use multiple computer or system to flood a targeted resources (Elleithy & Blagovic, 2006).

**2) Malicious software(Malware)**

Malware is short for malicious software which is developed by cyber criminals to destroy computer system and steal data (Aslan & Samet, 2020) For example: Viruses, Trojan Viruses and Spyware.

**3) Phishing**

It means a technique for attempting to obtain sensitive and important informations such as bank account numbers through a fraudulent web sites (Alkhalil et al., 2021).

**4) Advanced Peristent Threats(APTs)**

An advanced persistent threats (APTs) is a cover cyberattacks on a computer network where the attacker maintains unauthorized access to the targeted network and remains undetected for a specific time of period. (Mat et al., 2024) Cybercriminals continuously develop tools to deploy security technologies ,such as antiviruses and firewalls (Mat et al., 2024).

**5) Man-in-the-middle (MitM) Attacks**

Man-in-the-middle is a form of attack in which cyber criminals exploiting weak web-based protocols insert themselves between entities in communication channel to steal important information or data.it needs a communication channel to make a MitM attack (Mallik et al., 2019).

## 3. DEFINITION OF CYBER TERRORISM:

In (Iftikhar,2024) Cyber terrorism is defined as the use of internet-based attacks in terrorist activities, involving deliberate, large-scale disruption of computer networks through tools such as computer viruses, worms, phishing, and other malicious software, with the intention of causing significant harm and instilling fear and In (Vats,2017) Cyber terrorism is defined as the convergence of cyberspace and terrorism, involving the use of digital technologies to carry out terrorist activities aimed at causing disruption, fear, or harm, particularly targeting critical infrastructure, government systems, financial institutions, and essential services.

Combining this definition, Cyber terrorism is the deliberate use of internet-based attacks, utilizing tools such as computer viruses, worms, phishing, and other malicious software, to disrupt computer networks and critical infrastructure. It involves the convergence of cyberspace and terrorism, aiming to cause significant harm, instill fear, and target essential services, government systems, and financial institutions, with the intention of achieving political, ideological, or strategic objectives (Iftikhar,2024) (Vats,2017).

## 3.1 TYPES OF CYBER TERRORISM:

### 1) Defancement

Web defancement means an attack in which cyber criminals or hacker launch malicious code to web for modify or delete web page content or replace content with their own messages (Albalawi et al., 2022). Causes of defancement is weak server, no user awareness, weak administrator and no system updates (Albalawi et al., 2022).

### 2) Cyber Hostage-Taking

In cyber hostage cyber criminals make targets data unusable or to prevent access to computer system until a ransom is paid, usually in untracceable digital currency (Wade, 2021).

### 3) Cyber Stalking and Harassment

Cyber stalking is a crime when someone use internet and technologies for to harass or stalk another person online sending some unwanted frightening messages or emails (Pittaro, 2007). For ex: posting offensive or rude comments online, Releas confidential and sensitive information online.

## 4. REPRESENTATION OF WAREFARE CASE:

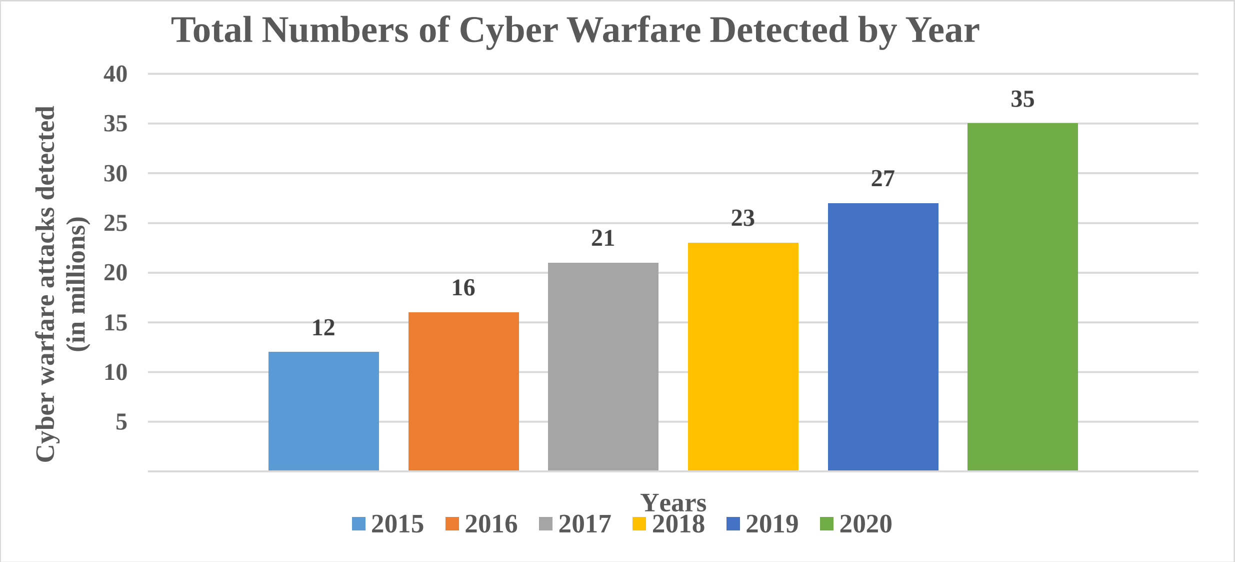

**Figure 4.1 shown about total numbers of cyber warfare detected by given below years**

In figure4.1, the total numbers of cyber warfare incidents detected by year from 2015 to 2020, combining data from both malware and phishing incidents (Alkhalil et al., 2021) (Talukder, 2020). In 2015, the total number of incidents detected was 125,937,500. This figure represents the baseline for the subsequent years. In 2016, the number of detected incidents rose to 163,930,000. In 2017, the upward trend continued with 213,335,000 incidents detected. By 2018, the detected incidents had further increased to 235,322,500. The continuous growth suggests an ongoing rise in both the frequency and sophistication of cyber threats. In 2019, the number of incidents detected reached 273,075,000. In 2020, the detected incidents surged to 359,586,000. The dramatic rise can be largely attributed to the COVID-19 pandemic, which led to an increase in remote work and online activities, thereby expanding the attack surface for cybercriminals and resulting in more frequent cyber warfare incidents. Overall, the chart illustrates a consistent and significant increase in cyber warfare incidents over the years, with a notable spike in 2020 due to the unique circumstances brought about by the pandemic.

## 5. REPRESENTATION OF CYBETERRORIM CASES:

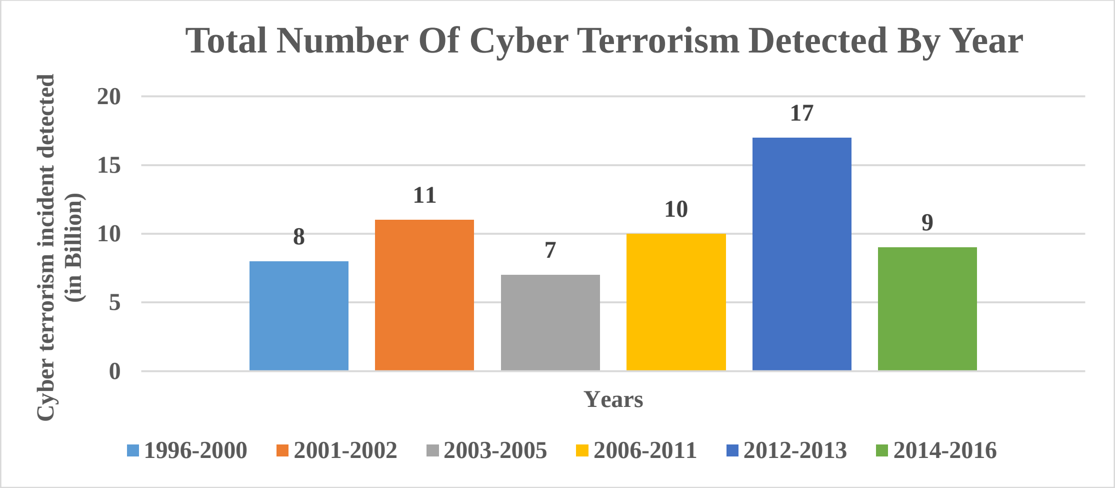

**Figure 5.1 shown about total numbers of cyber terrorism detected by given below years**

In figure5.1, the data highlights fluctuations in cyber terrorism detection, with notable increases during 2001-2002 and a peak in 2012-2013, followed by a decline in 2014-2016.The chart shows the number of cyber terrorism incidents detected per year, in billions, across different periods. From 1996-2000, 8 billion incidents were detected per year. This increased to 11 billion per year in 2001-2002, likely due to heightened global focus on security and counter-terrorism following the 9/11 attacks, leading to better detection and reporting mechanisms. The number dropped to 7 billion per year from 2003-2005, then rose to 10 billion per year from 2006-2011. A peak of 17 billion incidents per year was detected in 2012-2013, likely reflecting the growing sophistication and frequency of cyber attacks, along with enhanced detection technologies and increased awareness of cyber threats. Finally, from 2014-2016, 9 billion incidents were detected per year (Evren, 2020).

**Table 6.1 DIFFRENCE BETWEEN CYBER WARFARE AND CYBERTERRORISM**

| **Points** | **Cyber Warfare** | **Cyber Terrorism** |
|---|---|---|
| **Definition** | Cyberwarfare refers to the use of digital attacks by one nation-state to disrupt the computer systems of another nation-state. These attacks are typically conducted for strategic or military purposes, such as intelligence gathering, disruption of critical infrastructure, or undermining the adversary's defense capabilities (GOOD, 2015). | Cyber terrorism involves the use of digital attacks by non-state actors or terrorist groups to cause fear, disruption, or damage for ideological, political, or religious reasons. These attacks aim to terrorize populations, influence government policies, or achieve broader-ideological goals. (Iftikhar,2024) |
| **Purpose** | The primary goal is to cause losses to the enemy in the context of a war, whether ideological or declared (R43955, 2015). | The intent is to instill fear and harm among civilians, aiming to coerce or intimidate a government or |

| | | |
|---|---|---|
| | | civilian population (R43955, 2015). |
| **Target** | Typically involves state actors targeting critical infrastructure, military systems, or other national assets to weaken or destabilize an adversary.<br>(Ayers, 2004). | Often targets civilian infrastructure, such as communication systems, water supply, power grids, and transportation systems, to create widespread panic and disrupt everyday life (Ayers, 2004). |
| **Scope** | The focus is often on long-term strategic outcomes and can be a part of larger military operations (Ayers, 2004). | Targets can also include symbolic sites or events to maximize<br>Psychological impact<br>(Ayers, 2004). |
| **Example** | If an agent of a foreign power carries out an attack on another nation's infrastructure, it is considered cyber warfare. (R43955, 2015). | A cyber-attack intended to disrupt public services or infrastructure with the goal of causing fear among the population is classified as cyber terrorism (R43955, 2015). |

## 7. CONCLUSION:

In summary, Cyber warfare is primarily state- driven with strategic military goals, whereas cyber terrorism is conducted by non-state actors aiming to induce fear and achieve ideological .Cyber warfare is when countries attack each other's digital systems to gain an advantage, while cyber terrorism is when groups use digital attacks to create fear and chaos. Although they use similar methods to attack, their purposes are different. Both types of attacks exploit weaknesses in our digital systems, making them hard to defend against. Strong cybersecurity measures, global cooperation, and ongoing updates to defense strategies are crucial. Understanding these threats helps us protect our national security and public safety.

## REFERENCES:

**1.** Albalawi, M., Aloufi, R., Alamrani, N., Albalawi, N., Aljaedi, A., & Alharbi, A. R. (2022). Website Defacement Detection and Monitoring Methods: A Review. *Electronics (Switzerland)*, *11*(21). https://doi.org/10.3390/electronics11213573

**2.** Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. *Frontiers in Computer Science*, *3*(March), 1–23. https://doi.org/10.3389/fcomp.2021.563060

**3.** Aslan, O., & Samet, R. (2020). A Comprehensive Review on Malware Detection Approaches. *IEEE Access*, *8*, 6249–6271. https://doi.org/10.1109/ACCESS.2019.2963724

**4.** Ayers, M. C. (2004). *By Timothy O' Hara*. *U.S. Army War College, Carlisle Barracks, Carlisle, PA, 17013-5050*, 6.

**5.** Elleithy, K., & Blagovic, D. (2006). Denial of Service Attack Techniques: Analysis, Implementation and Comparison. *Journal of Systemics,* 3(1), 66–71. http://www.iiisci.org/Journal/CV$/sci/pdfs/P129065.pdf

**6.** Evren, A. G. (2020). Cyber Terrorism and Energy Security: A growing threats imperils entire regions. *Journal of European Security and Defence Issues*, *8*(May, 2018), 1 to 69.

**7.** GOOD, G. (2015). 済無No Title No Title No Title. *Angewandte Chemie International Edition, 6(11), 951–952.*, *1*(April).

**8.** Iftikhar, S. (2024). Cyberterrorism as a global threat: a review on repercussions and countermeasures. *PeerJ Computer Science*, *10*. https://doi.org/10.7717/peerj-cs.1772

**9.** Mallik, A., Ahsan, A., Shahadat, M. M. Z., & Tsou, J. C. (2019). Man-in-the-middle-attack: Understanding in simple words. *International Journal of Data and Network Science*, *3*(2), 77–92. https://doi.org/10.5267/j.ijdns.2019.1.001

**10.** Mat, N. I. C., Jamil, N., Yusoff, Y., & Kiah, M. L. M. (2024). A systematic literature review on advanced persistent threat behaviors and its detection strategy. *Journal of Cybersecurity*, *10*(1), 1–18. https://doi.org/10.1093/cybsec/tyad023

**11.** Pittaro, M. L. (2007). Cyber stalking : An Analysis of Online Harassment and Intimidation. *International Journal*, *1*(2), 180–197.

**12.** R43955. (2015). Cyberwarfare and Cyberterrorism: In Brief. *R43955*, 1–15. papers3://publication/uuid/F4C68E9F-5A04-4D5D-A4D8-0FE87699F347

**13.** Robinson, M., Jones, K., & Janicke, H. (2015). Cyber warfare: Issues and challenges. *Computers and Security*, *49*, 70–94. https://doi.org/10.1016/j.cose.2014.11.007

**14.** Talukder, S. (2020). *Tools and Techniques for Malware Detection and Analysis*. *February*. http://arxiv.org/abs/2002.06819

**15.** Vats, P. (2017). A comprehensive review of Cyber Terrorism in the current scenario. *2nd IEEE International Conference on Innovative Applications of Computational Intelligence on Power, Energy and Controls with Their Impact on Humanity, CIPECH 2016*, *c*, 277–281. https://doi.org/10.1109/CIPECH.2016.7918782

**16.** Wade, M. (2021). Digital hostages: Leveraging ransomware attacks in cyberspace. *Business Horizons*, *64*(6), 787–797. https://doi.org/10.1016/j.bushor.2021.07.014