iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** IV **Month of publication:** April 2026

DOI: https://doi.org/10.22214/ijraset.2026.79747

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue IV Apr 2026- Available at www.ijraset.com

Cyber Warfare: Issues and Challenges

Dr. Yogita Thareja[1], Angana Saini[2]
[1]*Assistant Professor, School of Information Technology, Vivekananda Institute of Professional Studies - Technical Campus, AU-Block, (Outer Ring Road), Pitampura, Delhi -110034, India*
[2]*Student, School of Information Technology, Vivekananda Institute of Professional Studies - Technical Campus, AU- Block, (Outer Ring Road), Pitampura, Delhi -110034, India*

Abstract: Cyberwarfare involves strategic digital strikes, such as malware, DDoS, and espionage, targeting a nation's critical infrastructure to cause significant disruption or physical harm. By compromising financial, military, and public systems, these attacks turn digital networks into a modern battlefield, as evidenced by incidents like Stuxnet and the Russia-Ukraine conflict. To counter these threats and maintain national stability, organizations must adopt proactive defense strategies, including Zero Trust architecture and advanced endpoint protection, to mitigate the risk of systemic collapse.

I. INTRODUCTION

Cyberwarfare is a series of strategic cyber attacks against a nation-state, causing it significant harm. This harm could include disruption of vital computer systems up to the loss of life. Cyberwarfare is typically defined as a set of actions by a nation or organization to attack countries or institutions' computer network systems with the intention of disrupting, damaging, or destroying infrastructure by computer viruses or denial-of-service attacks. And the hope is that effective cyber threat intelligence tools can reduce the harms done by these attacks.

II. WHAT IS CYBER WARFARE

Cyberwarfare causes equivalent harm to real warfare and breaks important computer systems. Some planned effects could be espionage. A country or organization's employment of computer viruses or denial-of-service attacks to target a country's or institution's computer network systems to interfere with, damage, or destroy infrastructure is known as cyber warfare.
Vital infrastructure like financial markets, military databases, national power grids, and cyber warfare attacks can destabilize a nation. This damage may result in the failure of major computer system

III. WHAT DOES CYBER WARFARE LOOK LIKE

Cyberwarfare can take many forms, but all of them involve either the destabilization or destruction of critical systems. The objective is to weaken the target country by compromising its core systems.
This means cyber warfare may take several different shapes:

1) Attacks on financial infrastructure
2) Attacks on public infrastructure, like dams or electrical systems
3) Attacks on safety infrastructure like traffic signals or early warning systems.
4) Attacks against military resources or organizations

IV. HOW DO CYBER WARFARE ATTACKS WORK

1) Viruses, computer worms, phishing, and malware may all slow down essential infrastructure.
2) Denial of Service attacks block authorized users from connecting to certain computer networks or hardware.
3) From organizations, authorities, and commercial enterprises, theft and hacking of vital information.
4) National security and stability are at risk from cyber espionage or malware that results in data theft.
5) Campaigns of cheating or propaganda are meant to seriously disrupt or create unrest.

V. CYBER WARFARE VS CYBER WAR

Cyberwarfare is different from cyber war in that cyberwarfare typically refers to the techniques used while engaging in cyber war. For example, a state-sponsored hacker may try to hack into the Bank of England as an act of cyber warfare while engaging in a cyberwar against England and its allies.

This reflects that cyber war defines the conflict at a national level, while cyberwarfare drives it forward through targeted digital strikes. The two are deeply connected, and together they turn civilian infrastructure into part of the battlefield, making daily life more vulnerable than ever. Such tactics reflect how nations no longer depend only on traditional battlefields. Instead, digital infrastructure like power grids, media outlets, and financial systems has become the new frontline. These attacks are designed to create disruption, spread fear, and weaken public trust, without a single soldier on the ground. It's challenging to detect them, and they can strike civilian systems directly. This poses a growing threat that demands strong defenses and constant vigilance.

VI. HISTORY AND EXAMPLES OF CYBER WARFARE CONFLICTS

In 2010, Stuxnet was used to inflict physical damage on an enemy's industrial systems. It was, reportedly, used against Iran's nuclear program. In March 2014, Russia launched a distributed denial-of-service (DDoS) attack on Ukraine and also crippled Ukraine's election commission.

In 2015, Chinese hackers stole millions of records from the United States' Office of Personnel Management (OPM). Also, in 2017, weaponized ransomware NotPetya was used to attack Ukraine.

A. Russia-Ukraine cyber warfare in 2022

The **Russia-Ukraine crisis** began in February 2022, and the war is also now happening in the cyber world. Let me tell you, FortiGuard Labs observed new viper malware being used to attack Ukrainian targets and installed on at least several hundred machines across Ukraine. Several Ukrainian organizations have also succumbed to attacks that employed the KillDisk and HermeticWiper malware strains, which appear to destroy data on devices.What's more, a copy of the Remote Manipulator System (RMS), a utilities software tool that enables remote control of devices, was being distributed in Ukraine via fake "Evacuation Plan" emails.

B. Attack on Sony

In 2014, Sony Pictures was crippled by a massive cyberattack following its release of The Interview, a satirical film about North Korea. Hackers stole and leaked sensitive company data, erased files, and disrupted operations. The FBI attributed the attack to North Korean state-backed groups, citing strong similarities to their past campaigns

C. Enemies of Qatar

In 2018, American fundraiser Elliott Broidy accused Qatar of orchestrating a cyber campaign to leak his emails and damage his reputation in Washington. The same attackers allegedly targeted more than 1,200 individuals considered "enemies of Qatar," including officials from Egypt, Saudi Arabia, and the UAE. The case reflected how cyber warfare tools are used in political and diplomatic battles.

D. Attacks on journalism and media in the US

Media outlets have been frequent victims of cyber warfare tactics. In 2013, Syrian Electronic Army operatives disrupted platforms like Twitter and The New York Times over perceived support for rebel groups. Hacker collective LulzSec defaced news websites and even managed to disrupt FBI servers in the United States. Let me tell you, this exposed the vulnerability of media and government systems.

VII. STRATEGIES AND STRENGTHEN READINESS AND RESPONSE TO CYBER WARFARE THREATS

1) Implement advanced endpoint protection: Endpoints are often the first targets of attackers. Advanced endpoint security adds proactive defenses that block malware before it can spread. This approach ensures that critical systems remain protected even if attackers attempt ransomware deployment.
2) Block phishing attempts early: Social engineering is a common tactic for state-sponsored attackers. Anti-phishing technologies can help prevent these attempts by blocking malicious links and attachments at the source.
3) Strengthen DDoS defenses: Disrupting key services is a common goal in cyber warfare campaigns. With the right DDoS protection, organizations can filter out malicious traffic while keeping legitimate services online. This helps governments, defense sectors, and civilian systems stay resilient during large-scale attacks.
4) Enforce strict access controls: Controlling who gets access to critical systems is one of the strongest defenses against cyber warfare threats. Zero trust network access (ZTNA) implements strict checks at every step, limiting the scope of attacker movement.

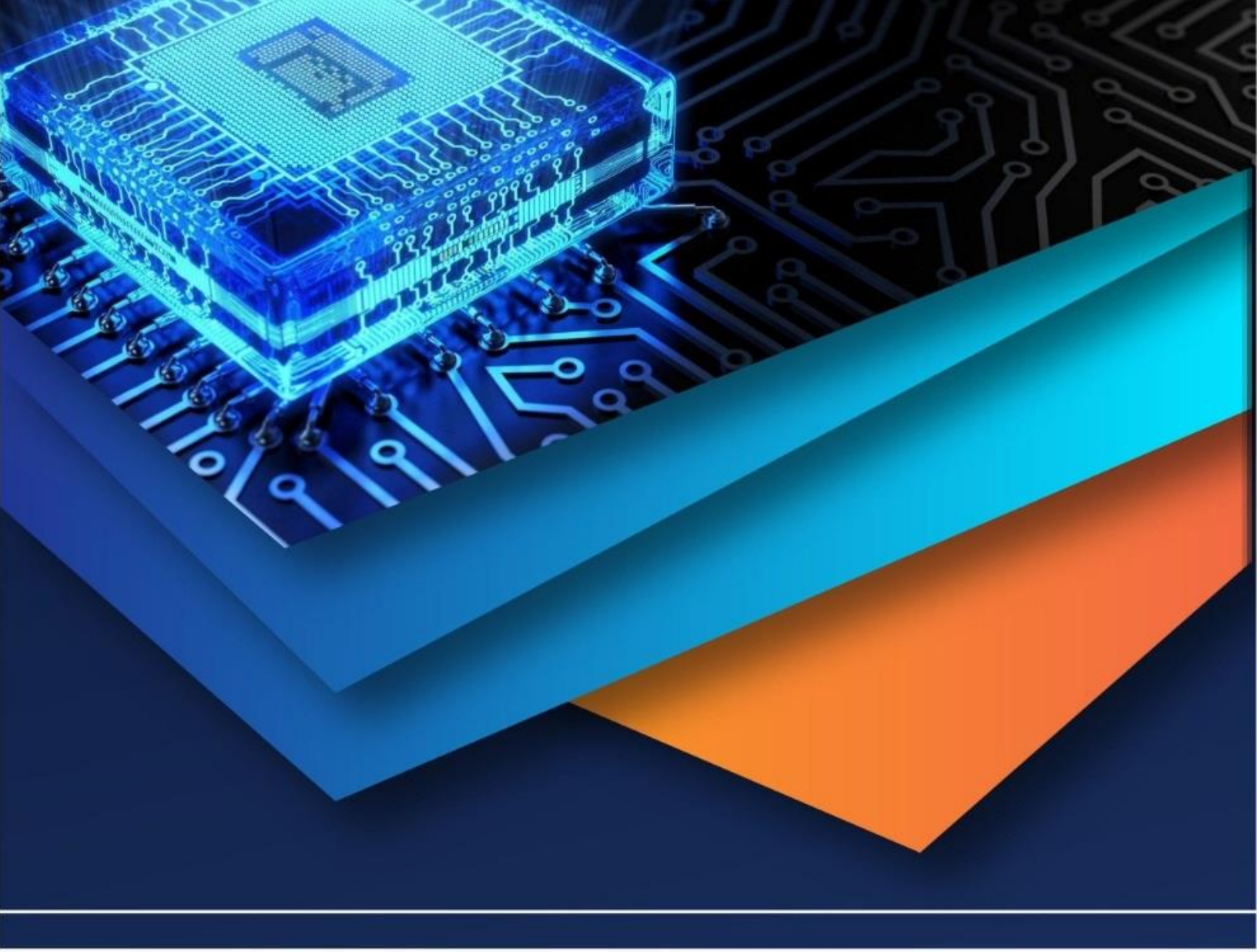
5) Data loss prevention (DLP): DLP solutions track how data moves within and outside the organization, identifying suspicious activity in real-time. They stop adversaries from exfiltrating classified or strategic information by halting unauthorized transfers.

VIII. CONCLUSIONS AND THOUGHTS FOR THE FUTURE

Cyberwarfare has fundamentally redefined the modern battlefield, shifting the focus from physical combat to the persistent destabilization of digital infrastructure. The distinction between cyberwar as a national state of conflict and cyberwarfare as the tactical execution of strikes highlights a future where civilian systems, from power grids to media outlets, are permanently on the front lines. Historical precedents like Stuxnet and the Russia-Ukraine crisis demonstrate that digital weapons now possess the power to cause physical destruction and societal unrest without a single soldier on the ground. Looking ahead, national security will depend less on traditional military might and more on the adoption of proactive, resilient frameworks such as Zero Trust Network Access and advanced endpoint protection. As digital threats become harder to detect and attribution remains complex, the survival of institutional trust and public safety will hinge on the continuous integration of sophisticated cyber threat intelligence. The future of global stability requires a shift toward constant vigilance, where defending civilian infrastructure is as critical as protecting military borders.

REFERENCES

[1] Fortinet. (n.d.). What is cyber warfare? Fortinet. https://www.fortinet.com/resources/cyberglossary/cyber-warfare
[2] GeeksforGeeks. (2024, February 21). What is Cyberwarfare? GeeksforGeeks. https://www.geeksforgeeks.org/computer-networks/what-is-cyberwarfare/
[3] Imperva. (n.d.). Cyber Warfare. Imperva. https://www.imperva.com/learn/application-security/cyber-warfare/
[4] Microsoft. (2022, February 28). Analysis of cyber threat activity in Ukraine. Microsoft Security Response Center. https://www.microsoft.com/en-us/msrc/blog/2022/02/analysis-resources-cyber-t hreat-activity-ukraine
[5] Zetter, K. (2014). Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. Crown. https://archive.org/details/countdowntozerod0000zett
[6] Federal Bureau of Investigation. (2014, December 19). Update on Sony Investigation. FBI. https://www.fbi.gov/news/press-releases/update-on-sony-investigation



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY