Online-Journals.org

iTDAF IETI Transactions on Data Analysis and Forecasting

iTDAF | eISSN: 2959-0442 | Vol. 2 No. 3 (2024) | OPEN ACCESS

https://doi.org/10.3991/itdaf.v2i3.51025

PAPER

Survey Paper on Cyber Warfare

Ahthasham Sajid(✉), Hamza Razzaq, Rida Malik, Arslan Ali Khan, Muhammad Sajid Iqbal, Sumaira Mushtaq

Department of Cyber Security, Riphah Institute of Systems Engineering, Riphah International University, Islamabad, Pakistan

ahthasham.sajid@riphah.edu.pk

ABSTRACT

Cyberspace warfare has emerged as a critical new front in national security, presenting complex challenges due to its multifaceted nature. This paper dissects cyber warfare across its physical, syntactic, and semantic layers, detailing common attack vectors such as reconnaissance, access, denial-of-service, and espionage. Motivations range from financial gain to political disruption, and attacks can take various forms, from preludes to conventional war to clandestine cold war tactics. Non-state actors such as cyber terrorists further complicate the landscape. Tools such as sniffers aid attackers, while firewalls offer some defense. The potential implications of cyberwar are stark, including disruption of essential services, economic damage, and national security threats. Understanding the ongoing discourse surrounding cyberwar, as reflected in the alarmist, skeptical, and realistic perspectives in the literature, is crucial for navigating this complex and evolving field.

KEYWORDS

DOS, DNS, Worms, ML

1 BACKGROUND

Operation Aurora, which started in China in 2006, was a targeted malware operation that took advantage of Internet Explorer zero-day vulnerability to target at least 30 significant companies, including Adobe and Google. The hack made it possible for malicious malware to infect users' PCs. Hackers appeared to have access to many software products' source codes. Five personnel of the People's Liberation Army's Unit 61398 were allegedly "assigned" to launch a widespread spear phishing (also known as "spear fishing") campaign with the goal of hacking into top US firms. Hackers targeted American trade secrets in this campaign, which primarily featured breaches at 141 corporations across 20 major industries between 2006 and 2014. For instance, Westinghouse is accused of stealing plans for specific types of nuclear power plants. This was the first time the term advanced persistent thread was coined [1]. The rise of cyber warfare marks a significant shift such as conflict, driven by the increasing reliance on digital technologies and the interconnectedness of global systems. Unlike traditional warfare, cyber warfare is conducted through the virtual

Sajid, A., Razzaq, H., Malik, R., Ali Khan, A., Iqbal, M.S., Mushtaq, S. (2024). Survey Paper on Cyber Warfare. *IETI Transactions on Data Analysis and Forecasting (iTDAF)*, 2(3), pp. 27–37. https://doi.org/10.3991/itdaf.v2i3.51025

Article submitted 2024-06-10. Revision uploaded 2024-08-01. Final acceptance 2024-08-02.

realm, targeting the critical infrastructure and information systems that modern societies depend on. This form of warfare leverages the anonymity and asymmetry of the cyber domain, allowing actors to engage in conflict without direct physical confrontation. Significant incidents in the history of cyber warfare, such as Stuxnet, the Ukraine power grid attacks, WannaCry, Not Petya, and the SolarWind breach, highlight the evolving nature of this threat. The Stuxnet worm, which targeted Iran's nuclear centrifuges, represents a milestone in the use of cyber weapons to achieve strategic objectives. It demonstrated the potential of cyber-attacks to cause physical damage to critical infrastructure [6]. The cyber-attacks on Ukraine's power grid in 2015 and 2016 demonstrated the potential for cyber warfare to disrupt critical infrastructure. These attacks caused widespread power outages and highlighted the vulnerabilities in national power systems [7]. The WannaCry and Not Petya ansomware attacks caused significant disruption and financial loss across multiple countries and industries. These attacks highlighted the global nature of cyber threats and the potential for widespread impact [8]. The SolarWind breach in 2020 compromised numerous US government agencies and private sector companies, underscoring the risks posed by supply chain vulnerabilities in software. This incident has been described as one of the most sophisticated and damaging cyber-attacks in recent history [9].

2 INTRODUCTION

Cyberspace has emerged as a new and critical domain of warfare, presenting unprecedented issues for national security and global stability. The digital age has ushered in a new era of conflict, one fought not on physical battlefields but within the complicated networks that underpin modern society. Cyber warfare, the use of cyber-attacks to disrupt, damage, or manipulate an enemy's critical systems, has emerged as a potent weapon in the arsenals of nation-states and non-state actors alike. This review paper delves into the current state of cyber warfare, exploring its evolving landscape, the growing sophistication of attacks, and the challenges faced by defenders. Cyber warfare has become an integral component of modern conflict, with its implications stretching across national security, international law, and global economic stability. Attackers may have diverse motivations, from straightforward financial gain through ransom demands to complex factors rooted in historical hostilities and religious beliefs. Understanding these motivations is crucial for comprehending the dynamics of cyber conflict [5].

2.1 Benefits of cyber warfare

Cyber warfare offers several strategic advantages for state actors, including asymmetry, deniability, and cost-effectiveness. It allows nations to engage in conflict without the use of conventional military force, potentially reducing casualties and infrastructural damage.

Asymmetry. Cyber warfare enables smaller states or non-state actors to challenge more powerful adversaries by exploiting vulnerabilities in critical infrastructure and information systems [10].

Deniability. The anonymous nature of cyber-attacks allow states to deny involvement, complicating attribution, and response efforts [11].

Cost effectiveness. Compared to traditional warfare, cyber-attacks can be conducted at a fraction of the cost, making it an attractive option for state and non-state actors alike [12].

2.2 Attacks over different layers

This section discusses the various types of attacks with respect to layers.

Attack on physical layer. Cyberwar involves some traditional warfare tactics, such as physical destruction of computers and networks, interference with communication channels, and compromise of human users, which pose significant threats. These attacks aim to gain physical access to networks or disrupt their operational integrity [2].

Attacks on syntactic layer. Cyber weapons that destroy, tamper with, corrupt, monitor, or otherwise harm the software running computer systems can be used to launch attacks on this layer. These weapons include malware, or malicious software such as worms, Trojan horses, spyware, and viruses that can infiltrate current software with corrupted code, allowing a computer to carry out operations that the user did not intend [2].

Attack on semantic layer. Semantic layer attacks also referred to as social engineering manipulate how human users perceive and interpret computer-generated data in order to fraudulently obtain sensitive user data, including passwords, bank account information, and classified government information. The most common social engineering approach is phishing, in which hackers send innocent-looking emails to specific recipients, asking them to reveal confidential information for what appear to be authentic intentions [2].

2.3 Characteristics of cyber war

Following are the main characteristics of cyberwar.

Organized. Attackers or hackers will employ a structured approach to penetrate the system with ease. They are able to obtain more effective results by employing procedures that are rationally ordered [4].

Enormous. When an attack is launched, the attackers typically operate on a massive scale, infecting almost billions of computers globally and resulting in massive data loss and financial damage [4].

Regimented. The attacks are planned in such a way that the harm they do is so great that it jeopardizes the organization's ability to function [4].

Not spontaneous or Ad Hoc. Attacks that are planned and executed with extreme precision in order to inflict the greatest amount of destruction [4].

Demanding time and resource. Since organizing an attack takes time and money, they will be prepared far in advance [4].

2.4 Forms of cyberwar

Cyber warfare encompasses various forms of attacks, each contingent on the adversary's objectives, motivations, and overall strategy. The nature of these attacks can range from converting actions exploiting the anonymity of the internet to overt attempts at disrupting critical infrastructure [5].

Cyberwar as prelude to conventional war. One strategic use of cyberwar is as a prelude to a real war. Attackers may launch cyber-attacks to cause disruption, confusion, and fear, aiming to diminish the targets will to fight and facilitate a quick capitulation. This approach parallels a traditional bombing campaign preceding a physical attack [5].

Cyberwar alongside conventional warfare. In certain scenarios, cyberwar is fought concurrently with conventional warfare. The focus is on targeting vital infrastructure, economic entities, and communication systems to disrupt the enemy's ability to effectively engage in the conflict [5].

Disruption of ally's response. Cyberwar tactics can extend to disrupting or slowing down an ally's response to a conventional attack against the intended target. For instance, launching cyber-attacks against the US before an attack on Taiwan could delay the American response, allowing the aggressor to establish control more effectively [5].

2.5 Cyber cold war dynamics

A cyber-cold war involves routine, clandestine attacks between adversaries, probing each other's systems and defenses. The anonymity of the internet allows for uncertainty in attribution, keeping the opposing side off balance without the risk of a conventional response [5].

Non-governmental actors in cyberwar. Cyberwar is not restricted to conflicts between governments. Organizations and cyber terrorist groups may engage in battles, launching attacks to create economic disruption and target entities perceived as adversaries [5].

Web account password cracking tool. An application downloaded from the Internet is used to "steal" a Yahoo email user's password. To access this email system, a user must input their password and user ID. Password entry appears to be reasonably secure. However, there is a method to go beyond the setup [3].

Sniffer tool. A sniffer on a network system is a software tool used to monitor network data. Sniffers can, however, also be employed as a tool for hacking hub-connected intranets. While some sniffers monitor TCP/IP traffic and filter out information in various formats, others give connection information such as TCP connection packets, bytes count, and interface statistics [3].

Service level network protection tool. One tool for preventing outside hackers from accessing a local area network is a firewall. Students get a firsthand look at the functioning and consequences of implementing a firewall during the cyberwar. It is not a "silver bullet," though. Certain popular ports are vulnerable to hacker attacks and must be kept open to the outside world [3].

2.6 Types of cyber attacks

This section discusses various latest types of attacks that could play a vital role in cyber warfare.

Reconnaissance attack. This kind of attack uses services and unapproved detection system mapping to steal data [4]. **Example:** packet sniffers, port scanning, ping sweeps and distributed network services (DNS) queries.

Access attack. It is an attack in which the perpetrator obtains access to a device that he is not authorized to use or access [4]. **Example:** port trust utilization, port redirection, dictionary attacks, man in the middle attacks, social engineering attacks and phishing.

Denial of services. Hacking into a system by turning off the network in order to prevent authorized users from using it [4]. **Example:** Smurf, SYN Flood, DNS attacks.

Cyber espionage. It is the act of using the internet to spy on others for gaining benefit of some sort [4]. **Example:** Tracking cookies, RAT controllable.

Passive attack. An attack that is mainly concerned with eavesdropping without meddling with the database [4]. **Example:** traffic analysis, release of message contents.

Active attack. An attack in which the attacker leaks the data transmission to all parties, thereby acting as a liaison and enabling severe compromise [4]. **Example:** masquerade, reply, modification of message.

Malicious attack. It is an attack that is caused for deliberately to cause severe harm resulting in large scale disruption [4]. **Example:** Sasser Attack.

Non-malicious attack. Accidental attack due to mishandling or operational mistakes with minor loss of data [4]. **Example:** registry corruption, accidental erasing of hard disk, network layer attacks, multi-layer attacks.

3 IMPLICATIONS OF CYBERWAR

The following are the implications of cyber warfare.

3.1 Disruption of essential services

Cyber-attacks can cripple critical infrastructure, potentially leading to blackouts, transportation delays, financial instability, and widespread chaos [2].

3.2 Economic impact

Businesses face substantial financial losses due to data breaches, intellectual property theft, and operational disruptions caused by cyber-attacks [2].

3.3 National security threats

Cyber warfare can compromise defense systems, disrupt military operations, and erode public trust in government institutions [2].

4 LITERATURE REVIEW

Cyberwar is characterized by a lack of consensus on its definition, reflecting the multifaceted nature of this evolving field. Since its emergence into public consciousness in the 1980s, scholars have grappled with diverse and sometimes contradictory perspectives, ranging from considering cyberwar as an imminent existential threat to skepticism about its classification as “war.” Hughes and Colarik’s cyberwar articles fail to offer explicit definitions. Three overarching themes—alarmist, skeptic, and realistic—pervade the literature, shaping discussions on the immediacy and nature of the cyberwar threat. Furthermore, the debate extends to the applicability of existing international law and norms to cyberspace, highlighting the need for a comprehensive framework that goes beyond traditional legal structures to address the unique challenges posed by cyber conflicts. This study examines the future of cyber warfare based on the collected recent studies, as illustrated via the research flow diagram in Figure 1. As technology continues to evolve, the potential consequences of cyber-attacks become increasingly severe. The authors in this study consider the need for international collaboration to develop frameworks and regulations = that govern the use of cyber weapons and mitigate the risks of escalation.

The latest research studies conducted on cyber warfare, along with their limitations and advantages, are highlighted in Table 1.

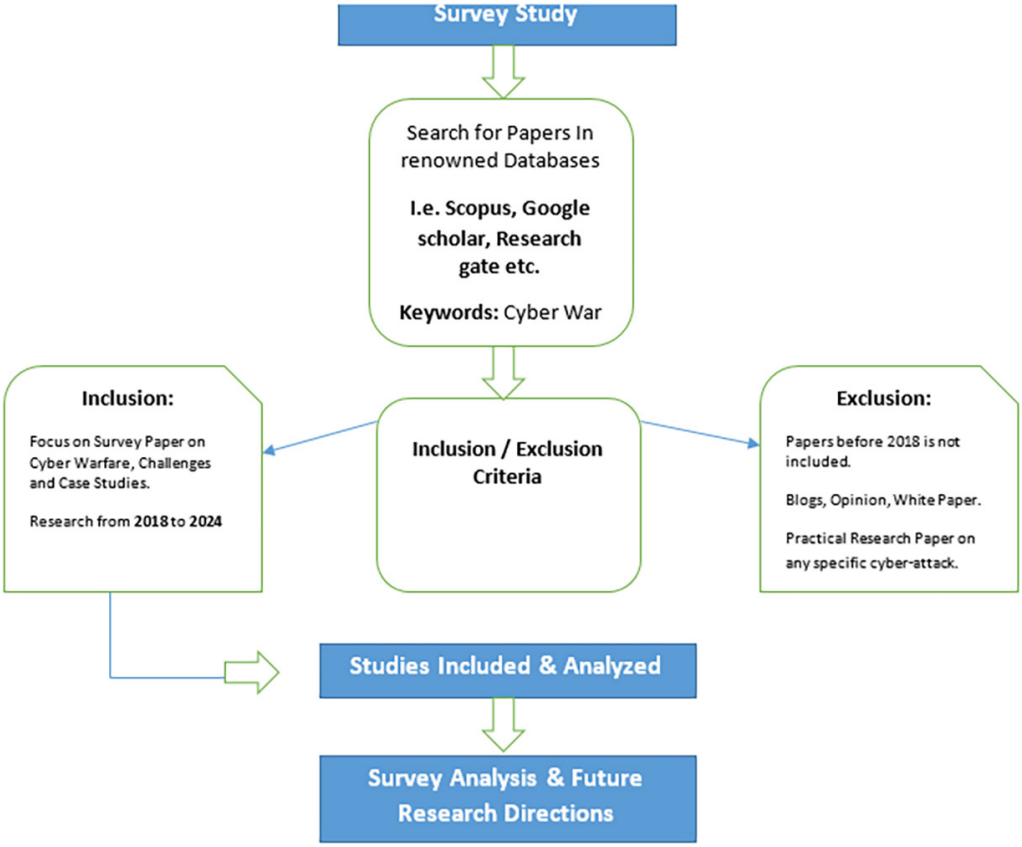

Fig. 1. Research flow of survey study

Table 1. Critical analysis

Year	Title	Problem	Advantages	Disadvantages
2023	Evolution of the Cyber Security Threat: An Overview of the Scale of Cyber Threat	The lack of integration of various perspectives and methodologies in addressing the evolving cyber security threats.	1) The paper provides a comprehensive overview of the evolution of cyber threats, shedding light on the increasing frequency and sophistication of cyber-attacks. It also focuses on the relationship between the levels of cyber security.	1) It lacks a systematic analysis of the standardization of cyber incidents like information collection, which could have provided a more in-depth understanding of cyber incidents threats towards different targets.
2023	A Survey on Various Cyber Attacks and Their Classification	Lack of understanding and knowledge about these attacks. The authors proposed a classification system to help people understand and defend against cyber-attacks.	1) Helps to identify the security goals that need to be met in order to protect against cyber-attacks.	1) Classification system are complex and can be difficult to understand. It is important to note that this system is not exhaustive and there may be new types of cyber-attacks that are not yet classified.
2022	INTEGRATE INFORMATION SECURITY WITH INTERNETWORKING	The lack of awareness of students on information security and the harmful effects it can have on us.	1) Highlights importance of information security and to teach students how to become sensitive about these issues 2) Works on how the percentages of internetworking and can be flexibly adjusted depending on students' reactions	1) This paper presents a nontraditional approach to incorporate the concept of information security. Traditionally, the course mainly concentrates on the interconnection of heterogeneous machines.

(Continued)

Table 1. Critical analysis *(Continued)*

2022	CYBER WAR	The main problem faced in the paper is the limited focus on the practical aspects of cyber warfare, such as the implementation of cyber deterrence ways.	1) The paper provides insights into the tactics and strategies employed in cyber warfare, shedding light on the evolving nature of warfare in the digital age.	1) The lack of emphasis on the importance of cyber education in the era of cyber war.
2021	The Birth of Cyber war	How a 2007 event in Esonia triggered the idea of cyber war and how this event continues to shape cyber security practices today	1) Helps us to understand how cyber security practices have changed since 2007.	1) It does not address all of the questions surrounding the emergence of cyber war.
2021	Defining cyber war: towards a definitional framework	Does not provide a single, universally accepted definition of cyber war to better understand it.	1) Provides a common ground for understanding the different perspectives on cyber war. 2) Provides information to develop new definitions of cyber war.	1) Does not provide a single, universally accepted definition of cyber war. 2) Can Prove to be too complex for some researchers.
2020	Information Warfare: Time for a redefinition	The main problem faced according to this paper is the difficulty in attributing attacks to specific actors. This makes it difficult to hold attackers accountable for attacks.	1) Highlights the key aspects of Espionage and propaganda which are still important aspects of information warfare, but the methods have changed with time.	1) The increasing vulnerability of critical infrastructure to attack is one of the biggest challenges in information warfare.
2020	THE TIMES OF CYBER ATTACKS	The increasing number of cyber-attacks and the financial losses they cause.	1) The advantages of highlighted in the article, are that cyber security can protect businesses and organizations from financial losses and data breaches.	1) The disadvantages, highlighted in this article, are that cyber security can be expensive and time-consuming to implement.
2020	CYBERWAR: FORMS AND EFFECTS	The article shows that cyber war is a serious threat that requires international cooperation to develop effective defense strategies and norms of behavior in cyberspace.	1) Relatively cheap and easy to carry out 2) Targeted attacks	1) Devastating effects on civilians 2) Unpredictable consequences
2020	National Cyber Security Strategy and the Emergence of Strong Digital Borders	The main problem faced in the paper is the lack of international cooperation and regulation in cyberspace, which is leading to an arms race between nation-states.	1) It provides a clear and concise overview of a complex issue that is cyber war. 2) It highlights some potential solutions, such as building trust and cooperation between countries, developing international norms and laws for cyberspace.	1) It does not adequately address the ethical implications of cyber warfare, such as the potential for civilian casualties and the erosion of privacy. 2) It is too short to provide a comprehensive analysis of a complex issue.

5 SURVEY ANALYSIS

The topic of cyberwar is a complex and multifaceted issue that needs proper attention for a better future. The implications of cyber warfare extend beyond the digital realm, affecting essential services, causing economic impacts, and posing national security threats. After carefully studying this issue, we have noted some of its characteristics. For example, when the cyberwar actually began, i.e., when

Operation Aurora took place in 2006, this operation, marked by the deployment of malware exploiting zero-day flaws and the involvement of military personnel, underscored the potential severity of cyber threats. We came across the layers that get attacked during a cyberwar and how they get attacked, i.e., the layers' physical, syntactic, and semantic of cyberspace highlight the diverse attack vectors, including traditional warfare tactics such as physical destruction, interference with communication channels, and compromise of human users. The types of attacks outlined range from reconnaissance and access attacks to denial of service and cyber espionage. We saw how attacks are planned and performed and what forms they take, i.e., the characteristics of cyber-attacks elucidate the organized, enormous, and regimented nature of these threats, emphasizing the deliberate planning involved. The different forms of cyber warfare, from motivations and objectives to cyber cold war dynamics, showcase the complexity and diversity of cyber conflicts.

The current landscape of cyber warfare presents both opportunities and challenges for state and non-state actors. The surveyed literature highlights several critical areas for future research and policy development:

5.1 Integration of advanced technologies

The use of artificial intelligence (AI) and machine learning (ML) in cyber operations offers significant potential for enhancing both offensive and defensive capabilities. However, there is a need for empirical studies to assess the real-world implementation and effectiveness of these technologies. Additionally, ethical guidelines and regulatory frameworks must be developed to govern their use.

5.2 Legal and ethical frameworks

The ambiguity in international law regarding cyber warfare remains a significant challenge. Future research should focus on developing comprehensive legal frameworks that address the complexities of cyber operations, including state responsibility and the rights of non-state actors. This includes creating clear guidelines for what constitutes an act of war in cyberspace and the appropriate responses.

5.3 Cyber resilience and critical infrastructure

Enhancing the resilience of critical infrastructure against cyber threats is paramount. The study should explore innovative approaches to public-private partnerships, the adoption of advanced threat detection technologies, and the implementation of continuous monitoring systems. Additionally, the development of standardized resilience metrics could help in assessing and improving the security posture of critical infrastructure.

5.4 Cyber deterrence strategies

Effective deterrence requires a combination of punitive measures, denial strategies, and international norms. Future studies should analyze successful case studies

of cyber deterrence and develop best practices that can be adopted by nations. Moreover, the role of cyber alliances and collective defense mechanisms in deterring cyber aggression should be explored.

5.5 Attribution and accountability

Improving the attribution of cyberattacks is crucial for holding perpetrators accountable and preventing future incidents. The study should focus on developing advanced forensic techniques and international collaboration mechanisms to enhance attribution capabilities. Additionally, establishing clear consequences for cyber aggression could deter potential attackers.

5.6 International collaboration and regulations

Foster international collaboration to establish clear regulations and norms governing cyber activities. Encourage nations to work together to create a unified approach to cyber security, sharing threat intelligence and best practices.

5.7 Investment in cyber security education and research

Increase investments in cyber security education and study to develop a skilled workforce capable of understanding and countering evolving cyber threats. Support academic institutions and training programs to stay ahead of cyber adversaries.

5.8 Enhanced cyber resilience

Implement measures to enhance cyber resilience across critical infrastructure sectors. This includes regular cyber security audits, threat simulations, and the development of contingency plans to ensure a rapid response in case of a cyber-attack.

5.9 Advanced threat detection and response

Invest in cutting-edge threat detection tools that can instantly recognize and neutralize online threats. Employ ML and AI techniques to examine network activity and identify irregularities that might point to a cyber-attack.

5.10 Global cyber security awareness campaigns

Launch global cyber security awareness campaigns to educate individuals, businesses, and government agencies about the risks of cyber threats. Promote best practices for online safety, including the importance of strong passwords and cautious behavior.

6 CONCLUSION

In conclusion, the rise of cyberspace as a battleground has ushered in a new era of warfare, presenting unprecedented challenges to national security and global stability. This multifaceted domain encompasses attacks on physical infrastructure, software systems, and human perception, employing diverse tactics such as reconnaissance, denial-of-service, and social engineering. Motivations range from financial gain to geopolitical disruption, while the forms of cyber warfare span a spectrum from covert espionage to overt attempts to cripple critical infrastructure. Understanding the characteristics, tools, and implications of cyber warfare is crucial for developing effective defenses and navigating the complex dynamics of this evolving threat landscape. The ongoing debate surrounding the definition, legality, and potential consequences of cyberwar underscores the urgent need for international cooperation and the development of robust frameworks to ensure stability and security in the digital age.

The studies reviewed in this paper highlight the dynamic and complex nature of cyber warfare, emphasizing the need for continued study and international cooperation. The integration of advanced technologies, the development of robust legal and ethical frameworks, and the enhancement of cyber resilience are essential steps toward mitigating the risks associated with cyber conflicts. By addressing these challenges, the international community can work towards a more secure and stable cyberspace.

7 REFERENCES

[1] S. Geol, "National cyber security strategy and the emergence of strong digital borders," *Connections*, vol. 19, no. 1, pp. 73–86, 2020. https://doi.org/10.11610/Connections.19.1.07

[2] P. Brahmanand and A. Ospanova, "Cyber war," *International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET),* vol. 11, no. 4, pp. 3454–3462, 2022. https://www.ijirset.com/upload/2022/april/15_CYBER_NC.pdf

[3] C. D. Yang, "Integrate information security with internetworking," in *32nd ASEE/IEEE Frontiers in Education Conference*, 2002. Available at: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=797b6d89dbda3df574d16f0b28c50b6074a46f2c (Accessed: 24 December 2023).

[4] M. Uma and G. Padmavathi, "A survey on various cyber attacks and their classification," *International Journal of Network Security*, vol. 15, no. 5, pp. 390–396, 2013. Available at: http://ijns.jalaxy.com.tw/contents/ijns-v15-n5/ijns-2013-v15-n5-p390-396.pdf

[5] R. Finnegan, "Cyberwar: Forms and Effects," *Issues in Information Systems*, vol. 21, no. 1, pp. 290–300, 2020. https://doi.org/10.48009/1_iis_2020_290-300

[6] R. Lee, "Stuxnet: A case study in cyber warfare," *Cyber Defense Review*, vol. 7, no. 1, pp. 78–89, 2018.

[7] T. Brown, "Cyber attacks on Ukraine's power grid," *Journal of Critical Infrastructure Protection*, vol. 6, no. 4, pp. 145–156, 2020.

[8] S. Wilson, "The global impact of WannaCry and NotPetya," *International Journal of Cyber Threats*, vol. 7, no. 2, pp. 345–356, 2019.

[9] L. Green, "The SolarWinds incident: A comprehensive analysis," in *Conference on Cyber Incident Response*, 2020, pp. 67–78.

[10] J. Smith, "The asymmetric nature of cyber warfare," *Journal of Cyber Security*, vol. 5, no. 2, pp. 123–134, 2020.

[11] M. Johnson, "Deniability in cyber attacks: Challenges and strategies," in *International Conference on Cyber Defense*, 2019, pp. 45–56.
[12] R. Lee, "Cost-effectiveness of cyber operations," *Cyber Security Review*, vol. 4, no. 1, pp. 78–89, 2018.

8 AUTHORS

Ahthasham Sajid is with the Department of Cyber Security, Riphah Institute of Systems Engineering, Riphah International University, Islamabad, Pakistan (E-mail: ahthasham.sajid@riphah.edu.pk).

Hamza Razzaq is with the Department of Cyber Security, Riphah Institute of Systems Engineering, Riphah International University, Islamabad, Pakistan.

Rida Malik is with the Department of Cyber Security, Riphah Institute of Systems Engineering, Riphah International University, Islamabad, Pakistan.

Arslan Ali Khan is with the Department of Cyber Security, Riphah Institute of Systems Engineering, Riphah International University, Islamabad, Pakistan.

Muhammad Sajid Iqbal is with the Department of Cyber Security, Riphah Institute of Systems Engineering, Riphah International University, Islamabad, Pakistan.

Sumaira Mushtaq is with the Department of Cyber Security, Riphah Institute of Systems Engineering, Riphah International University, Islamabad, Pakistan.