International Journal of Computer and Communication Technology

Volume 9
Issue 1 *Research on Computing and Communication Sciences.*

Article 5

July 2023

Security Life Cycle framework for Exploring & Prevention of Zero day attacks in Cyberterrorism

Bassam Mohammad Elzaghmouri Dr.
Jerash University, el_zaghmouri@yahoo.com

Ahmad khader Habboush Dr.
Jerash University, ahmad_ram2001@jpu.edu.jo

Security Life Cycle framework for Exploring & Prevention of Zero day attacks in Cyberterrorism

Bassam Mohammad Elzaghmouri[1] ,Ahmadkhader habboush[2]

[1]Department of Computer Science, Faculty of Computer Science and Information Technology, Jerash University, Jerash, Jordan

b.el-zaghmouri@jpu.edu.jo

[2]Department of Computer Networks, Faculty of Computer Science and Information Technology, Jerash University, Jerash, Jordan

ahmad_ram2001@jpu.edu.jo

Abstract

The rise of cyber terrorism poses a significant threat to governments, businesses, and individuals worldwide. Cyber terrorists use information technology to carry out attacks that range from simple hacking attempts to more sophisticated attacks involving malware, ransom ware, and zero-day exploits. This paper aims to provide an in-depth understanding of cyber terrorism, with a special focus on zero-day attacks. As the world becomes more digitized and automated, it brings convenience to everyone's lives. However, it also leads to growing concerns about security threats, including data leakage, website hacking, attacks, phishing, and zero-day attacks. These concerns are not only for organizations, businesses, and society, but also for governments worldwide. This paper aims to provide an introductory literature review on the basics of cyber-terrorism, focusing on zero-day attacks. The paper explores the economic and financial destruction caused by zero-day attacks and examines various types of zero-day attacks. It also looks at the steps taken by international organizations to address these issues and the recommendations they have made. Additionally, the paper examines the impact of these externalities on policymaking and society. As cyber-security becomes increasingly important for businesses and policymakers, the paper aims to delve deeper into this aspect, which has the potential to threaten national security, public life, and the economic and financial stability of developed, developing, and underdeveloped economies.

Keywords: Cyber-terrorism, zero-day attacks, Ransom ware, Phishing, Digitization, Security threats

1. Introduction

Cyber terrorism involves the use of technology, specifically information and computer systems and networks, to conduct acts of terrorism. Cyber terrorists use various malicious methods such as hacking, cyber-attacks, malware distribution, D DoS attacks, and digital sabotage to cause widespread fear, panic, disruption, or damage to critical infrastructure, economies, or societies. They can target government agencies, financial institutions, healthcare facilities, transportation systems, communication networks, and other critical infrastructure. Cyber terrorism can be motivated by political, ideological,

religious, or financial reasons. It poses a significant threat to national security, public safety, and economic stability, resulting in significant losses, such as sensitive data disruption, essential services disruption, financial loss, and potential loss of life. Cyber-terrorism is a growing concern worldwide, with increasing digitization and automation leading to a rise in security threats such as zero-day attacks, ransom ware, and phishing. As organizations, businesses, and society become more reliant on information technology, they are becoming more vulnerable to cyber-attacks that can cause economic and financial destruction. This paper aims to provide a comprehensive understanding of cyber-terrorism, with a specific focus on zero-day attacks, ransom ware, phishing, and other security threats in a digitized world. We will explore the types and motives behind these attacks, the potential impact on targeted systems, and the challenges involved in detecting and mitigating them. Additionally, we will examine the steps taken by international organizations to address these issues and the recommendations they have made. Finally, we will explore the impact of these externalities on policymaking and society and the importance of effective cyber security measures to protect against cyber-terrorism.

2.Related Work

The use of digital and cyberspace to cause harm, instill fear, and further a political, social, or economic agenda is known as cyber terrorism. In recent decades, cyber terrorism has become an increasingly significant threat to national security, attracting more attention from practitioners, scholars, and politicians. This literature review aims to provide an overview of how the current expansion of the internet has made network security a critical concern for both businesses and government organizations. Although the internet offers numerous benefits, there is also a significant risk of being hacked, which can offset these advantages. Additionally, the amount of data being stored and shared online continues to grow, resulting in a higher risk of security breaches. One particular type of security breach is known as a "zero-day" attack. This review provides an overview of cyber terrorism, including its definitions, characteristics, motivations, tactics, impact, and countermeasures. Although there is no universally accepted definition of cyber terrorism, researchers define it based on their perspectives. Alharbi (2019) provides an in-depth understanding of the definitions, motives, and impact of cyber terrorism. They also discuss different types of cyber terrorism attacks and the methods used by cyber terrorists. The review concludes with a discussion of the challenges in countering cyber terrorism. Halderman (2017) discusses the issue of responsible disclosure of zero-day vulnerabilities, which are a type of cyber terrorism attack that exploits previously unknown vulnerabilities in software. The authors provide an overview of the different types of zero-day vulnerabilities and the challenges in detecting and disclosing them. They also discuss the ethical considerations in responsible disclosure. According to Denning (2000) and Weimann (2004), cyber terrorism is the use of cyberspace by non-state actors to create chaos or anarchy by inflicting harm to people, property, or critical infrastructure for political, ideological, or financial purposes. Studies by Arquilla and Ronfeldt (1997) and Stohl (2007) suggest that cyber terrorism is a

form of information warfare or a subset of terrorism that achieves similar goals through cyber space. Cyber terrorism can be characterized by the utilization of advanced technology, the potential for anonymity and remote attacks, the exploitation of vulnerabilities in digital systems, and the intent to spread fear and disrupt society. Various sectors, such as government, military, financial institutions, energy, transportation, communication systems, and critical infrastructure, can all be targeted by cyber terrorists. Cyber terrorists might have a variety of objectives, and it can be difficult to pin down their exact goals. According to some academics, political, ideological, or religious objectives are the primary drivers of cyber terrorism. These motivations attempt to advance a specific agenda, undermine the status quo of power, or denounce perceived injustices (Weimann, 2004; Denning, 2010). Others contends that financial gain, including extortion, fraud, or the theft of sensitive data, can be a driving force behind cyber terrorism (Cherdantseva, Burnap, et al., 2016; Conway, 2018).

Cyber terrorists can use a wide variety of ways to carry out their assaults. Malware attacks, distributed denial-of-service (DDoS) attacks, social engineering scams, insider threats, and other cutting-edge techniques for gaining unauthorized access, upsetting systems, stealing data, or causing harm are some examples of these. To incite fear, panic, and misinformation, cyber terrorists may also use psychological manipulation, propaganda, and social media.

3. Zero Day Attacks

A zero-day attack is a type of cyber attack that exploits a previously unknown vulnerability or weakness in a software or system. Zero-day attacks are often considered the most dangerous type of cyber attack because they can be used to target systems and networks that are otherwise secure, and there may be no patch or fix available to address the vulnerability. This makes zero-day attacks particularly attractive to cyber criminals and state-sponsored hackers. To mitigate the risks of zero-day attacks, it is important for organizations to implement strong cyber security measures, such as regularly updating software and systems, using firewalls and intrusion detection systems, and conducting regular security audits. Additionally, it is important to have a plan in place for responding to a zero-day attack, which includes identifying, and isolating the affected systems, notifying users and stakeholders, and working with security experts to develop a patch or fix to address the vulnerability. It is also important for software vendors and developers to implement secure coding practices and conduct regular security testing to identify and address vulnerabilities before they can be exploited by attackers. Finally, collaboration and information sharing between security researchers, vendors, and organizations can help to identify and address zero-day vulnerabilities more quickly, reducing the risks of a successful attack.

There are several types of zero-day attacks that cybercriminals can use to exploit previously unknown vulnerabilities in software or systems. Here are some of the most common types of zero-day attacks:

1. Remote code execution (RCE): This type of attack involves exploiting a vulnerability in a software or system to execute malicious code remotely, giving the attacker control over the affected system.

2. Denial-of-service (DoS): In a DoS attack, the attacker floods the target system or network with traffic, causing it to become overwhelmed and unavailable to users.
3. Privilege escalation: A privilege escalation attack involves exploiting a vulnerability to gain elevated access to a system or network, allowing the attacker to execute code or install malware with greater privileges.
4. Browser exploits: Browser exploits take advantage of vulnerabilities in web browsers to execute malicious code and compromise the security of a system or network.
5. Watering hole attacks: In a watering hole attack, the attacker compromises a website or web application that is frequently visited by the target organization or individual, allowing them to launch a targeted attack.
6. File less attacks: A file less attack involves exploiting vulnerability in a system or network without leaving any files or traces behind. Instead, the attacker uses scripts or other techniques to execute malicious code in memory.
7. Memory exploits: Memory exploits take advantage of vulnerabilities in software or system's memory management to execute malicious code and gain control over the affected system.

4. Methodology

The Security Life Cycle is a framework that outlines the steps involved in securing an information system throughout its life cycle. The steps involved in the Security Life Cycle are as follows:

1. Security Policy Creation: The first step in the Security Life Cycle involves creating a security policy. A security policy outlines the organization's security objectives and the procedures and guidelines that employees should follow to ensure the security of the information system.

2. Security Assessment: The second step involves conducting a security assessment to identify potential vulnerabilities and weaknesses in the information system. This may involve using tools and techniques to identify potential risks, such as penetration testing or vulnerability scanning.

3. Planning: Once the security assessment has been completed, the next step involves planning how to implement the necessary security measures. This may include identifying the resources required, developing a timeline for implementation, and determining the roles and responsibilities of those involved in implementing the security measures.

4. Threat/Risk Assessment: The fourth step in the Security Life Cycle is to conduct a threat and risk assessment. This involves identifying potential threats to the information system and the likelihood and impact of those threats. Based on this

assessment, organizations can determine the level of security measures that are required.

5. Policy Enforcement/ Implementation: The fifth step involves enforcing the security policy and implementing the necessary security measures. This may involve implementing technical measures such as access controls, firewalls, and intrusion detection systems, as well as non-technical measures such as employee training and awareness programs.

6. Intrusion Detection: The sixth step involves implementing intrusion detection systems. Intrusion detection systems can help to detect and prevent unauthorized access to the information system.

7. Manage/Monitor: The final step in the Security Life Cycle involves managing and monitoring the security of the information system over time. This includes regular monitoring and maintenance to ensure that the system remains secure and protected from potential threats.

By following the Security Life Cycle, organizations can ensure that their information systems remain secure and protected from potential threats throughout their life cycle.

Figure 1: The Security Life Cycle

5.Issues and Challenges of Cyber terrorism on zero-day attacks

Cyber terrorism with a special focus on zero-day attacks raises several issues that need to be addressed by organizations and governments. Here are some of the key issues:

1. Legal and Ethical Concerns: Zero-day attacks can be used to cause harm to individuals, organizations, and even governments. This raises legal and ethical concerns about the use of these attacks, particularly if they are used for criminal or terrorist purposes.
2. Impact on Critical Infrastructure: Zero-day attacks can have a significant impact on critical infrastructure, such as power grids, transportation systems, and financial institutions. This can result in widespread disruption and damage, as well as a significant financial impact.
3. National Security Implications: Zero-day attacks can be used to target national security assets, including military and government systems. This raises concerns about the potential for cyber terrorism to be used as a weapon of war, and the need for strong national security measures to protect against these attacks.
4. Economic Impact: Zero-day attacks can result in significant economic damage, particularly for organizations that rely on digital systems and networks to conduct their operations. This can result in lost revenue, damaged reputation, and other negative impacts.
5. Privacy Concerns: Zero-day attacks can be used to steal sensitive information, including personal and financial data. This raises privacy concerns about the use of these attacks and the need to protect personal information from unauthorized access.
6. Cyber security Skills Shortage: Zero-day attacks require a high level of technical expertise to develop and execute. This highlights the need for organizations and governments to invest in cyber security training and education to address the growing skills shortage in this field.

Cyber terrorism with a special focus on zero-day attacks presents several challenges for organizations and governments. Here are some of the key challenges:

1. Difficulty in Detection: Zero-day attacks are designed to exploit previously unknown vulnerabilities, making them difficult to detect using traditional security measures. This makes it challenging for organizations to protect against zero-day attacks, as they may not know that vulnerability exists until it has been exploited.
2. Lack of Preparedness: Many organizations are not prepared to respond to zero-day attacks, as they may not have the necessary tools, technologies, or expertise to detect and mitigate the attack. This can result in extended downtime and data loss, as well as reputational damage.
3. Complexity of Attack Techniques: Zero-day attacks are often complex and sophisticated, requiring a high level of technical expertise to develop and execute. This makes it challenging for organizations to defend against these attacks, as they may not have the same level of technical expertise or resources as the attackers.
4. Rapid Proliferation: Zero-day

attacks can spread quickly, as attackers seek to exploit vulnerabilities across multiple systems and networks. This can result in widespread disruption and damage, as well as a significant financial impact.

5. Limited Information Sharing: There is often limited information sharing between organizations and governments about zero-day attacks, as organizations may not want to disclose vulnerabilities for fear of exploitation. This can limit the ability of organizations and governments to prepare and respond to these attacks effectively.
6. Increasing Sophistication of Attackers: Attackers are becoming increasingly sophisticated in their use of zero-day attacks, making them more challenging to detect and defend against. This requires organizations to continually adapt and enhance their security measures to keep pace with the evolving threat landscape.

6.Analysis, Detection, and Prevention Techniques of cyber terrorism with Zero Attacks

Cyber terrorism is defined as the use of computer technology to create fear, panic, and disruption for political or ideological purposes. Zero-day attacks refer to the exploitation of previously unknown vulnerabilities in software or hardware systems. These attacks can be particularly damaging because there is no patch or update available to fix the vulnerability. In this response, we will discuss analysis, detection, and prevention techniques for cyber terrorism on zero-day attacks.

6.1 Analysis

Cyber terrorism is a serious threat to national security and critical infrastructure, and zero-day attacks are particularly concerning due to their ability to exploit previously unknown vulnerabilities in software and hardware systems.

Zero-day attacks refer to the exploitation of vulnerabilities that are unknown to software vendors, making them particularly difficult to detect and prevent. These attacks can be launched by state-sponsored actors, terrorist groups, or cybercriminals for political, ideological, or financial gain. Zero-day attacks are particularly concerning because they can be used to steal sensitive data, disrupt critical infrastructure, or launch widespread cyber attacks.

To analyze cyber terrorism with a special focus on zero-day attacks, we need to understand the tactics, techniques, and procedures (TTPs) used by attackers. This involves studying the types of attacks used, the vulnerabilities that are commonly exploited, and the tools and techniques used by attackers.

State-sponsored actors are among the most significant threats when it comes to cyber terrorism and zero-day attacks. These actors often have extensive resources and access to sophisticated hacking tools, making them difficult to detect and prevent. In addition, these attackers may have political or ideological motivations, making their attacks particularly challenging to predict.

Terrorist groups may also use cyber terrorism as a means of achieving their goals. These groups may use zero-day attacks to disrupt critical infrastructure or steal sensitive data, causing fear and panic among the public. Cybercriminals may also

use zero-day attacks to steal valuable information or launch ransom ware attacks for financial gain.

To prevent zero-day attacks, organizations must take a proactive approach to cyber security. This includes implementing strong access controls, keeping systems and software up to date with the latest patches and updates, implementing network segmentation to limit the impact of an attack, and conducting regular security audits and risk assessments. Organizations should also use threat intelligence feeds to stay up to date with the latest threats and implement machine learning and artificial intelligence tools to identify and respond to anomalies.

However, cyber terrorism is a serious threat that requires a proactive and multidimensional approach to detect and prevent. With a special focus on zero-day attacks, organizations need to stay vigilant and implement a range of measures to reduce the risk of an attack and respond quickly and effectively if one does occur.

6.2 Detection

Detecting cyber terrorism with a special focus on zero-day attacks is critical to preventing these attacks from causing harm. Zero-day attacks exploit previously unknown vulnerabilities, making them difficult to detect and prevent. In this we will discuss the detection of cyber terrorism with a special focus on zero-day attacks.

1. Implement Intrusion Detection and Prevention Systems: Intrusion detection and prevention systems (IDPS) monitor network traffic for signs of an attack. IDPS can detect and alert security teams to potential zero-day attacks, giving them time to respond and prevent the attack from causing harm.
2. Use Advanced Threat Intelligence: Advanced threat intelligence provides real-time information on the latest threats, including zero-day attacks. This helps organizations stay ahead of potential attacks and implement security measures to prevent them.
3. Conduct Regular Security Audits and Risk Assessments: Regular security audits and risk assessments can identify vulnerabilities and threats, including those associated with zero-day attacks. This helps organizations stay ahead of potential attacks and implement security measures to prevent them.
4. Implement User and Entity Behavioral Analytics (UEBA): UEBA uses machine learning algorithms to detect anomalies in user behavior that may indicate an attack. UEBA can detect zero-day attacks that may go unnoticed by other security measures.
5. Use Sandboxing: Sandboxing involves isolating applications or processes in a secure environment to detect and analyze potential threats. Sandboxing can detect zero-day attacks by analyzing the behavior of unknown applications or processes.
6. Implement Continuous Monitoring: Continuous monitoring involves monitoring networks and systems in real-time to detect and respond to potential threats. This includes using security information and event management (SIEM) tools to monitor and analyze logs from network devices, servers, and applications.

However, detecting cyber terrorism with a special focus on zero-day attacks requires a proactive and multi-layered approach. Organizations should implement intrusion detection and prevention systems, use advanced threat intelligence, conduct

regular security audits and risk assessments, implement user and entity behavioral analytics, use sandboxing, and implement continuous monitoring. These measures help organizations detect potential zero-day attacks and respond quickly to prevent them from causing harm.

6.3 Prevention

Preventing cyber terrorism with a special focus on zero-day attacks requires a multi-layered approach that involves implementing a range of security measures to reduce the risk of an attack. The prevention of cyber terrorism with zero-day attacks are :

1. Implement Strong Access Controls: Implementing strong access controls is crucial in preventing cyber terrorism. This includes implementing two-factor authentication, password policies, and least privilege access, which limits user access to only what, is necessary for their job functions.
2. Keep Systems and Software Up-to-Date: Keeping systems and software up-to-date is essential in preventing zero-day attacks. Software vendors release patches and update to address vulnerabilities and it is essential to implement them promptly. Implementing a patch management process is necessary to ensure timely updates.
3. Implement Network Segmentation: Network segmentation limits the impact of an attack by separating the network into smaller, more secure segments. By limiting access between segments, the attack can be contained, and the damage is reduced.
4. Conduct Regular Security Audits and Risk Assessments: Regular security audits and risk assessments identify vulnerabilities and threats and provide a roadmap for implementing security measures. This helps organizations stay ahead of potential threats and reduce the risk of cyber terrorism.
5. Use Machine Learning and Artificial Intelligence: Machine learning and artificial intelligence (AI) are powerful tools in detecting and responding to zero-day attacks. These technologies can detect anomalies and patterns that indicate an attack, and can respond quickly to minimize the damage.
6. Implement Threat Intelligence Feeds: Threat intelligence feeds provide real-time information about the latest threats, including zero-day attacks. This helps organizations stay ahead of potential attacks and implement security measures to prevent them.

However, preventing cyber terrorism with a special focus on zero-day attacks requires a proactive and multi-layered approach. Organizations should implement strong access controls, keep systems and software up-to-date, implement network segmentation, conduct regular security audits and risk assessments, use machine learning and AI, and implement threat intelligence feeds. These measures help organizations stay ahead of potential threats and reduce the risk of cyber terrorism.

7. Impact on Policy Making and Society

Zero-day attacks refer to cyber attacks that exploit previously unknown vulnerabilities in software or hardware systems. Cyber terrorism on zero-day attacks can have a significant impact on policy making and society in various ways:

I. National Security: Zero-day attacks

pose a severe threat to national security, especially if they are used for cyber terrorism. These attacks can target critical infrastructure, such as energy, transportation, and communication networks, which could disrupt essential services and cause widespread panic.

II. Economic Impact: Zero-day attacks can also have a significant economic impact by causing financial losses to businesses, damaging intellectual property, and disrupting supply chains. This can result in lost revenue, lost jobs, and a decrease in consumer confidence, which can have a negative effect on the economy.

III. Policy Making: Cyber terrorism on zero-day attacks can influence policy-making decisions. Governments may implement stricter regulations, impose sanctions on countries or groups involved in cyber terrorism, or increase funding for cyber security research and development.

IV. Public Perception: The impact of zero-day attacks on society can also influence public perception. If a significant attack occurs, people may lose faith in the government's ability to protect them, resulting in increased anxiety and fear. This can lead to calls for increased surveillance and security measures, which may infringe on civil liberties.

V. International Relations: Zero-day attacks can also impact international relations, particularly if the attacks are attributed to a foreign government or group. This can result in diplomatic tensions, trade restrictions, or even military action.

However, cyber terrorism on zero-day attacks can have far-reaching impacts on policy-making and society, and it is crucial for governments and businesses to take proactive steps to prevent and mitigate these types of attacks

8. Recommendation

Cyber terrorism with a special focus on zero-day attacks is a constantly evolving threat that requires organizations to remain vigilant and proactive in their approach to cyber security. In addition to prevention and detection measures, there are several recommendations that organizations can implement to mitigate the risk of zero-day attacks.

1. Develop a Comprehensive Cyber security Strategy: A comprehensive cyber security strategy should be developed and implemented to address the organization's specific risks and vulnerabilities. The strategy should include policies, procedures, and training programs to ensure all employees are aware of the risks and their role in protecting the organization.

2. Engage in Regular Training and Awareness Programs: Regular training and awareness programs should be conducted to ensure all employees are aware of the latest threats and how to identify potential zero-day attacks.

3. Implement Incident Response Plans: Incident response plans should be developed and tested to ensure the organization can respond quickly and effectively to a cyber attack. The plan should include procedures for detecting, containing, and mitigating the impact of a zero-day attack.

4. Regularly Backup Data and Systems: Regularly backing up data and systems can help organizations recover quickly in the event of a zero-day attack. Backups should be stored offsite or in the cloud to ensure they are not impacted by the attack.

5. Develop Partnerships with Security Vendors and Government Agencies: Organizations should develop partnerships with security vendors and government agencies to stay informed of the latest threats and receive guidance on how to mitigate the risk of zero-day attacks.

6. Conduct Regular Penetration Testing: Regular penetration testing can identify vulnerabilities that may be exploited in a zero-day attack. Penetration testing should be conducted by a third-party provider to ensure unbiased results.

9. Conclusion

The paper looks at the literature review of cyber-terrorism with special focus on zero-day attacks. With growing digitalization across all sectors and industries globally, cyber threats and vulnerability has now become one of the major concerns of all organizations. This issue has gained high significance with the top management and is an essential agenda item for governance and ethics of the organization. It has implications for all of us and may have various motivations aligned with personal, political, religious, financial and others. The paper is a preliminary work of understanding cyber world in terms of security, terrorism, attacks, hacking with special focus on zero-day attacks. We intend to take this work further with more understanding of the increasing impact of this domain and its impact on all the spheres of business and society including policy making by the governments at all local, regional, national and global levels. We also intend to extend this work to understand how the lesser known space of cyber-security is being significant to national security, public life, economic and financial stability as the sensitive data gets accumulated in various forms ofdigitalizedmechanismstherebyassuminghighestlevelofsafehavenapparatusesfordeveloped,developing and even under-developing economies.

References

[1] Gaylah, K. D.,& Vaghela, R. S. (2023). Mitigation and Prevention Methods for Distributed Denial-of-Service Attacks on Network Servers. In *Advancements in Smart Computing and Information Security: First International Conference, ASCIS 2022, Rajkot, India, November 24–26,, R* (pp. 70-82). Cham: Springer Nature Switzerland.

[2] Alharbi, S., & Venter, H. S.

(2019). A systematic review of cyber terrorism. Computers & Security, 84, 226-243.

[3] Halderman, J. A., & Waters, B. (2017). Zero-day vulnerabilities and responsible disclosure. Proceedings of the IEEE, 105(7), 1239-1246.

[4] Arquilla, J., Ronfeldt, D. "Cyberwar is coming!" In Athena's camp: Preparing forconflictintheinformationage,Edited byArquilla,J.,Rnfeldt,D,24-60,SantaMonicaCA: RAND (1997).

[5] Ashraf, C, Defining cyberwar: Towards a definitional framework, Defense & SecurityAnalysis,37(3), 274-294(2021).

[6] Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., Stoddart, K,A review of cyber security risk assessment methods for SCADA systems, Computers& Security, 56, 1-27 (2016).

[7] Conway, M. Reality bytes: Cyberterrorism and terrorist 'use' of internet, DCU OnlineResearchAccess Service, (2002)

[8] Conway,M.,Iscyberterrorismareal threat?–Yes(2018)https://doras.dcu.ie/22241/1Pro-Cyberterrorism_Ch_Doras_Version.pdf,LastaccessedonApril25,2023.

[9] Daud, M., Raisah, R., George, M., Asirvatham, D, Thangiah, G. Bridging the gapbetweenorganisationalpracticesand cybersecuritycompliance:Cancooperationpromote compliance in organizations? International Journal of Business and Society,19(1),161-180 (2018)

[10] Denning,D.Cyberterrorism:Thelogicbombversusthetruckbomb,GlobalDialogue,Nicosia, 2(4),29-37 (2000).

[11] Denning D. Terror's web: How the internet is transforming terrorism, Handbook of Internet Crimes, 194-213(2010).

[12] Franklin,O.,Ismail,M.Thezero-dayvulnerability,InternationalJournalofInformationSystem and Engineering, 9(1), 65-76,(2021).

[13] Halder,D.,InformationTechnology Actandcyberterrorism:Acriticalreview, CentreforCyberVictimCounselling, 2011.https://ssrn.com/abstract=1964261

[14] Holt, T., Stonhouse, M, Freilich, J., Chermak, S, Examining ideologically motivated cyber attacks performed by far-left groups, Terrorism and Political Violence (2018),DOI:10.1080/09546553.2018.1551213.

[15] https://www.trendmicro,com/en_us/devops/22/I/zero-day-threat-protection.html,lastaccessedon April 24, 2023.

[16] Lee, C., Choi, K., Shandler, R., Kayser, Mapping global cyber terror networks; AnempiricalstudyofAl-QaedaandISISCyberterrorism,JournalofContemporaryCriminalJustice. (Forthcoming)

[17] Kilger, M. Anticipating the nature and likelihood of a cyber terror community, CyberInfrastructureProtectionVolumeIII,StrategicStudiesInstitute.USArmyWarCollege,2017.

[18] PenemonSullivanPrivacyReportMay2020.https//ponemonsullivanreport.com/2020/05.Last accessed on April 25, 2023.

[19] Rattray, G ,Strategic War farein Cyberspace, MIT Press,2001

[20] Samuel,K.,Osman,W.Cyberterrorismattachofthecontemporaryinformationtechnology age: Issues, consequences and panacea, International Journal of

Computer Science and Mobile Computing, 3(5), 1082-1090 (2014).
[21] Sankardas, P., Raeez, M., Baby, B. Ethical hacking: Impacts on society, InternationalJournal of Advanced Research in Computer and Communication Engineering, 9(1),212-215(2020).
[22] Stohl, M. Cyber terrorism: A clear and present danger, the sum of all fears, breakingpointor patriot games?Crime, Law andSocial Change, 46(4-5),223-238 (2007).
[23] SymantecIntelligenceReport,August2015,SymantecCorporationWorldHeadquarters,CA 94043,USA.
[24] Weimann,G.Cyberterrorism:How realisthethreat?.(2004).
[25] What is zero-day attack? – Definition and explanations,https://www.kaspersky.co.in/resource-center/definitions/zero-day-exploit,last accessedon April 24,2023.
[26] Sarhan, M., Layeghy, S., Gallagher, M., & Portmann, M. (2023). From zero-shot machine learning to zero-day attack detection. *International Journal of Information Security*, 1-13.
[27] Peppes, N., Alexakis, T., Adamopoulou, E., & Demestichas, K. (2023). The Effectiveness of Zero-Day Attacks Data Samples Generated via GANs on Deep Learning Classifiers. *Sensors*, *23*(2), 900.
[28] Javaheri, D., Gorgin, S., Lee, J. A., & Masdari, M. (2023). Fuzzy Logic-Based DDoS Attacks and Network Traffic Anomaly Detection Methods: Classification, Overview, and Future Perspectives. *Information Sciences*.
[29] Rath, M., & Pattanayak, B. K. (2019). Security protocol with IDS framework using mobile agent in robotic MANET. *International Journal of Information Security and Privacy (IJISP)*, *13*(1), 46-58.
[30] Pattanayak, B. K., Pattnaik, O., & Pani, S. (2020). A novel approach to detection of and protection from Sybil attack in VANET. In *Advances in Intelligent Computing and Communication: Proceedings of ICAC 2019* (pp. 240-247). Springer Singapore.
[31] Swain, J., Pattanayak, B. K., & Pati, B. (2017, March). Study and analysis of routing issues in MANET. In *2017 international conference on inventive communication and computational technologies (ICICCT)* (pp. 506-509). IEEE.