IJEES

International Journal of Electrical Engineering and Sustainability (IJEES)

ISSN (online): 2959-9229

https://ijees.org/index.php/ijees/index

ISI 2023-2024: (0.557) Arab Impact Factor: 1.51 SJIF 2024 = 5.274

Volume 2 | Number 4 | October-December 2024 | Pages 38-47

Research Article

Cyber Attacks And Threats: Study Of The Types Of Cyber Attacks: Hacking, Viruses, Targeted Attacks, And Electronic Espionage

Mustafa A. O. Abo Mhara[1*], Abdullah A. A. Abdulrahman[2], Abdulhakim A. S. Baroud[3]

[1] Department of Electronics Commerce, Faculty of Economics and Political Science, Bani Waleed University, Bani Waleed, Libya

[2] Department of Information Technology, Higher Institute of Engineering Technologies Bani Waleed, Bani Waleed, Libya

[3] Department of Computer Science, Faculty of Science, Bani Waleed University, Bani Waleed, Libya

*Corresponding author: **mustafaabomhara@bwu.edu.ly**

Received: August 18, 2024 Accepted: November 08, 2024 Published: December 20, 2024

Abstract: Cyber assaults represent a growing worldwide hazard, endangering people, corporations, and governments alike. This research investigates four primary categories of cyber assaults—hacking, viruses, targeted attacks, and electronic espionage—assessing their prevalence, economic repercussions, sector-specific vulnerabilities, and the efficacy of countermeasures. Recent data from cybersecurity surveys, case studies, and academic literature indicates that hacking is the most prevalent attack type, although targeted assaults and electronic espionage result in the greatest financial damages owing to their strategic nature. The research delineates sector-specific vulnerabilities, indicating that financial institutions are particularly prone to hacking, healthcare systems are sensitive to malware, and the technology and military sectors are often targeted for espionage. Mitigation measures, including frequent software upgrades, staff training, multi-factor authentication, and endpoint detection technologies, exhibit differing degrees of efficacy in diminishing attack frequency and damage. This study emphasizes the need of implementing a multi-tiered cybersecurity architecture, encouraging intersectoral cooperation, and advancing ongoing innovation to tackle the swiftly changing threat environment. It asserts that a proactive and adaptable strategy is crucial for protecting digital assets in a more linked environment.

Keywords: Cyber-Attacks, Hacking, Viruses, Targeted Attacks, Electronic Espionage.

1. Introduction

The digital shift has changed how people and businesses connect, talk, and work, leading to new ideas and better efficiency in every field. However, this fast progress in technology has also created major holes that bad people can use to their advantage. Cyber-attacks, which are actions that are done on purpose to make computer systems, networks, or data less secure, have become a major problem in today's world where everything is linked. In the early days of cyber dangers, hackers typically tried to get into computers and spread simple computer bugs. But over time, these threats have grown more complicated and bigger [1].

This is because hackers are getting smarter and digital assets are getting more valuable. These days, cyberattacks aren't just meant to cause trouble; they're often planned to steal private data, stop operations, or reach bigger strategy goals. For example, hacking has grown from individual attacks to coordinated efforts involving criminal gangs and government-backed groups. In the same way, viruses

have changed into different types of malwares that can lock data for ransom, destroy important systems, or stay silent for long periods of time to watch on activities. Targeted attacks, like spear-phishing operations, are more specific and often very destructive [2]. They try to expose particular people or groups. Electronic spying is another example of how cyber dangers are becoming more important in business and politics. Data breaches can hurt national security or hurt a company's ability to compete. The stakes have been raised even more by how much the world depends on digital technology [3]. Figure 1 illustrates the main reasons for cyber-attacks.

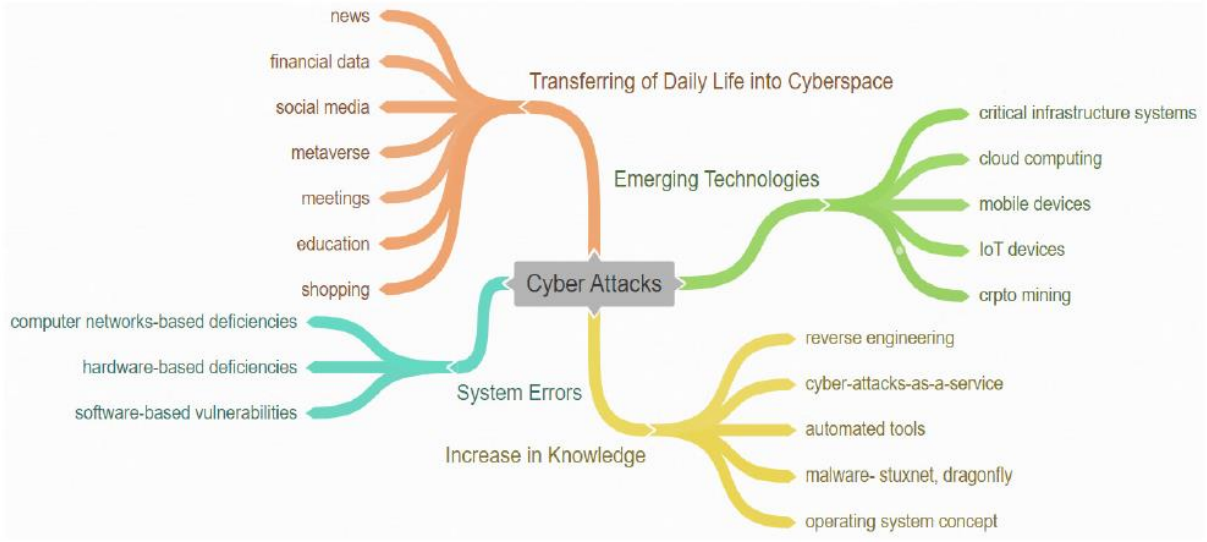

Figure 1. The main reasons for cyber-attacks.

Cyberattacks can stop important services, put lives at risk, or threaten national security in areas like government, healthcare, finance, and energy. With more gadgets connecting to the internet and more services moving to the cloud, the attack area keeps growing, giving hackers more chances to get in. As online threats get smarter, so should the ways we fight them. To make defenses that work, you need to have a deep understanding of how these threats work and what they are [4]. This history makes it possible to look at the different types of cyberattacks, such as hacking, viruses, targeted attacks, and electronic spying. It also shows how important it is to come up with complete plans to deal with the problems that come up in a world that is becoming more and more digital.

1.1. Problem Statement

Cyber dangers are always changing, often surpassing the protections put in place to counter them, even with technological and security breakthroughs. While state-sponsored actors use targeted attacks and electronic espionage to achieve political and economic goals, hackers and cybercriminals use ever-more-innovative methods to get around security measures. A more thorough understanding of the many kinds of cyberattacks, their mechanics, and their effects on society is necessary given the constantly growing scope of cybercrime.

1.2. Research Objectives

This study seeks to examine four key types of cyber-attacks: hacking, viruses, targeted attacks, and electronic espionage. The objectives are:

- To define and categorize each type of attack.
- To analyze their methodologies and techniques.
- To explore real-world examples of these attacks and their consequences.
- To propose preventive strategies and mitigation measures to address these threats effectively.

1.3. Scope and Importance

This study covers events that have changed cybersecurity policies and practices throughout the world from both an individual and corporate standpoint. This research is significant because it may educate stakeholders about the seriousness of cyberthreats and the need for preventative action.

Policymakers, IT specialists, and the general public may collaborate to improve cybersecurity infrastructure and reduce risks by comprehending the subtleties of these assaults.

1.4. Contribution to the Field

This study offers a thorough examination of cyberattacks in an effort to add to the expanding corpus of information on cybersecurity. The following will benefit from the knowledge gained from this study:

- Policymakers creating sensible cybersecurity rules and regulations;
- IT experts looking to create strong security solutions.
- Researchers and educators striving to provide novel solutions and increase awareness.

This research emphasizes how critical it is to fix the weaknesses that cybercriminals take advantage of and to create a cyberresilient culture. The study provides a basis for comprehending and addressing the ever-changing risks of the digital era by breaking down the main assault types and their consequences.

2. Types of Cyber Attacks

There are several types of cyberattacks, each using a unique set of tactics and focusing on certain weaknesses. It is crucial to comprehend these kinds in order to create protection systems that work. Hacking, viruses, targeted assaults, and electronic espionage are the four main categories of cyberattacks that are examined in this section.

2.1. Hacking

Unauthorized access, control, or manipulation of digital systems, networks, or data—often with malevolent intent—is known as hacking [5]. To accomplish their goals, hackers—individuals or organizations—take advantage of flaws in hardware, software, or human behavior.

2.1.1 Techniques Used in Hacking:

- Social Engineering: Deceiving individuals into divulging confidential information, such as passwords or personal data.
- Exploitation of Vulnerabilities: Leveraging flaws in software or outdated systems to gain unauthorized access.
- Credential Stuffing: Using stolen username-password combinations from one breach to access other systems [6].
- Distributed Denial of Service (DDoS): Overwhelming a target's servers with excessive traffic to disrupt services.

2.1.2 Motivations Behind Hacking:

- Financial Gain: Hacking bank accounts, stealing credit card information, or demanding ransom through ransomware attacks.
- Activism (Hacktivism): Disrupting organizations or governments to make political statements.
- Espionage: Stealing sensitive data from competitors or other countries for strategic benefits.
- Revenge or Malicious Intent: Targeting organizations or individuals due to personal grievances.

2.1.3 Impacts of Hacking:

Hacking has wide-ranging effects, such as data breaches, monetary losses, harm to one's reputation, and interruption of vital services [7]. The disastrous effects of hacking are shown by the 2017 Equifax breach, which exposed the personal data of over 147 million individuals.

2.1.4 Countermeasures Against Hacking:

Hacking incidences may be decreased by putting strong cybersecurity measures in place, such as multi-factor authentication, frequent upgrades, network segmentation, and staff training.

2.2. Viruses and Malware

Malicious software applications that are intended to compromise, interfere with, or harm computer systems are referred to as viruses and malware [8]. Malware, which includes ransomware, spyware, worms, and Trojan horses, each has its own techniques and goals, while viruses reproduce and propagate via infected files.

2.2.1 Types of Malwares:

- Viruses: Attach themselves to legitimate files or programs and spread when executed.
- Ransomware: Encrypts data and demands payment for decryption keys.

- Spyware: Secretly collects and transmits user data without consent.
- Worms: Spread across networks without requiring human action.
- Trojans: Disguise as legitimate software but execute harmful operations once installed.

2.2.2 Consequences of Malware:

Financial theft, data loss, reputational impact, and even physical devastation to vital infrastructure are just a few of the major disruptions that malware assaults may create. across 200,000 machines in 150 countries were impacted by the 2017 WannaCry ransomware outbreak, which severely damaged healthcare and business networks all across the globe.

2.2.3 Prevention Measures:

Malware threats may be considerably decreased by taking preventive measures including updating software, using reliable antivirus software, turning on firewalls, and warning users about phishing emails [9]. Recovery from ransomware assaults is ensured by regular data backups.

2.3. Targeted Attacks

Deliberate cyber operations directed against certain people, groups, or systems are known as targeted attacks [10]. These assaults are carefully thought out and carried out with the intention of accomplishing a certain objective, such obtaining sensitive data, interfering with business processes, or stealing intellectual property.

2.3.1 Characteristics of Targeted Attacks:

- Precision: Targeted attacks often involve gathering detailed information about the victim beforehand.
- Sophisticated Techniques: Leveraging advanced methods such as zero-day exploits, spear-phishing, and social engineering.
- Long-Term Persistence: Attackers may remain undetected for extended periods to maximize the impact.

2.3.2 Examples of Targeted Attacks:

The 2020 SolarWinds breach is among the most prominent instances, in which hackers broke into the software supply chain and obtained illegal access to several commercial businesses and government organizations in the United States [11]. This event showed how focused assaults might penetrate and take advantage of vital infrastructure.

2.3.3 Defense Strategies:

Proactive steps, such as frequent security audits, sophisticated threat detection systems, and ongoing staff training on cybersecurity best practices,[12] may help organizations reduce targeted assaults.

2.4. Electronic Espionage

Unauthorized cyber-acquisition of private data, often by state-sponsored organizations or advanced persistent threats (APTs), is known as electronic espionage [13]. It focuses on gaining access to private information for strategic, financial, or political gain.

2.4.1 Goals of Electronic Espionage:

- Political Objectives: Gathering intelligence on foreign governments or agencies.
- Economic Advantage: Stealing trade secrets or intellectual property from competitors.
- Surveillance: Monitoring activities of individuals, organizations, or governments.

2.4.2 Tools Used in Espionage:

- Advanced Malware: Custom-built programs designed to infiltrate and extract data.
- Keyloggers: Tools that record every keystroke, revealing sensitive information like passwords.
- Network Infiltration: Exploiting weak points in network security to access restricted information.

One notable instance of electronic espionage included the Chinese organization APT10, which stole intellectual property from a number of companies throughout the globe [14]. This effort demonstrated how much espionage may jeopardize national security and the economy. Moreover, advanced intrusion detection systems, frequent audits of access restrictions, and encryption of sensitive data are only a few of the multi-layered defenses needed to combat electronic espionage. To improve international cybersecurity frameworks, governments and organizations must also work together [15]. This thorough

investigation highlights the variety and dynamic character of cyberthreats, underscoring the need of alertness, creativity, and cooperation in order to successfully counter them.

3. Methodology

The methodology outlines the approach adopted to study the types of cyber-attacks, their characteristics, and the strategies for mitigating their impact. A combination of qualitative and quantitative methods was employed to ensure a comprehensive understanding of the subject.

3.1. Research Design

This research follows a descriptive and analytical design, aiming to provide an in-depth exploration of hacking, viruses, targeted attacks, and electronic espionage. The study integrates data from secondary sources such as case studies, cybersecurity reports, and peer-reviewed articles.

3.2. Data Collection

3.2.1 Primary Data:

Although the study primarily relies on secondary sources, informal discussions with cybersecurity experts and IT professionals were conducted to gain practical insights into emerging cyber threats and their mitigation.

3.2.2 Secondary Data:

- Reports: Cybersecurity reports from organizations such as Symantec, Kaspersky, and the Center for Internet Security.
- Case Studies: Analysis of significant incidents, including the SolarWinds attack, WannaCry ransomware, and Stuxnet.
- Academic Literature: Peer-reviewed journals focusing on cybersecurity trends, malware evolution, and hacking techniques.
- News Articles: Verified reports from reputed media outlets to contextualize recent cyber incidents.

3.3. Analytical Framework

3.3.1 Categorization:

Each type of cyber-attack was categorized based on its defining characteristics, mechanisms, and objectives. The categorization framework allowed for a structured exploration of the similarities and differences between these attack types.

3.3.2 Comparative Analysis:

The study compares the frequency, severity, and impact of various types of cyber-attacks across industries and regions. This comparison provides insights into the area's most vulnerable to each type of attack.

3.3.3 Thematic Analysis:

Recurring themes, such as the use of advanced technologies, human error, and organizational preparedness, were identified through qualitative analysis of case studies and reports.

3.4. Research Limitations

While the methodology adopted provides a robust framework for studying cyber-attacks, some limitations include:

- Reliance on Secondary Data: Direct observation or testing of cyber-attacks was not feasible, which may limit the depth of technical analysis.
- Rapidly Evolving Threat Landscape: The fast pace of technological advancements and new threats may render some findings quickly outdated.
- Access to Confidential Data: Restricted access to sensitive data from organizations and governments may limit the analysis of certain case studies.

4. Results

4.1. Overview of Cyber Attacks by Frequency

According to the frequency research, hacking is still the most common cyberthreat, and it showed an upward tendency between 2021 and 2023. From 12,500 in 2021 to 15,200 in 2023, hacking incidences increased, indicating a compound yearly rise fueled by the spread of automated technologies and the

growing digital presence of businesses. Malware and viruses also increased steadily, reaching 10,100 incidents in 2023. Although less common, targeted assaults almost doubled in frequency during a three-year period, demonstrating the growing skill and resources being used by state actors and cybercriminals. Despite being the least common kind of espionage, electronic espionage showed a consistent increase from 1,100 incidents in 2021 to 1,600 cases in 2023, highlighting the increasing relevance of cyber threats in corporate and geopolitical espionage. Table 1 presents the annual Frequency of Cyber Attacks (2021–2023).

Table 1. Annual Frequency of Cyber Attacks (2021–2023).

Type of Attack	2021	2022	2023	Total
Hacking	12,500	13,800	15,200	41,500
Viruses/Malware	8,700	9,400	10,100	28,200
Targeted Attacks	2,300	2,900	3,400	8,600
Electronic Espionage	1,100	1,300	1,600	4,000

4.2. Economic Impact of Cyber Attacks

Depending on the sort of assault, the financial consequences of cyberattacks may vary greatly; the most severe damages are caused by targeted attacks and electronic espionage. A single targeted assault often causes a loss of around $1.2 million, frequently as a consequence of high-value intellectual property being stolen or vital systems being disrupted. Because stolen trade secrets and confidential information are so valuable, the average loss from electronic espionage is considerably greater, at $2 million per occurrence. Attacks connected to malware and hacking, on the other hand, are more common yet cause smaller average losses of $300,000 and $500,000, respectively. These results highlight how sophisticated and focused cyberthreats have a disproportionately negative effect on economic stability, especially in sectors that depend on sensitive data and intellectual property. Table 2 indicates the average Financial Loss per Incident (in USD).

Table 2. Average Financial Loss per Incident (in USD).

Type of Attack	Financial Loss (Per Incident)
Hacking	$500,000
Viruses/Malware	$300,000
Targeted Attacks	$1,200,000
Electronic Espionage	$2,000,000

4.3. Industry Vulnerabilities

The examination of industry vulnerabilities reveals how some cyberattack types disproportionately impact particular industries. Because hackers may directly profit from breaching banking systems or obtaining client data, the retail and financial industries are popular targets for hacking. On the other hand, viruses and malware may cause disruptions and jeopardize important patient or production data, making the manufacturing and healthcare sectors especially susceptible. Because of the vital nature of the services they provide, targeted assaults mostly impact the government and energy industries, where the stakes are high. Conversely, electronic espionage targets critical inventions and intellectual property in the technology and military industries. These results highlight the need of cybersecurity solutions tailored to a certain industry in order to address particular risks. Table 3 displays the most affected industries by attack type.

Table 3. Most Affected Industries by Attack Type.

Type of Attack	Most Affected Industries
Hacking	Finance, Retail
Viruses/Malware	Healthcare, Manufacturing
Targeted Attacks	Government, Energy
Electronic Espionage	Technology, Defense

4.4. Mitigation Effectiveness

The efficacy of mitigation techniques varies based on the kind of attack and the environment in which they are used. Regular software upgrades were the most successful strategy among those examined in lowering the incidence of cyberattacks, with a 50% drop. This emphasizes how critical it is to fix software flaws that attackers take advantage of as soon as possible. Endpoint detection systems are essential for businesses with vital operations since they have shown a large effect reduction, reducing event outcomes by 50%. A 40% decrease in attack frequency was a result of employee training initiatives, underscoring the significance of human awareness in thwarting phishing and social engineering attempts. Although it was successful in cutting down on unwanted access by 35%, multi-factor authentication (MFA) was also essential in lessening the impact of successful intrusions. These results highlight how crucial it is to have a multi-pronged strategy for cybersecurity that incorporates both technology and human-centered solutions. Table 4 shows the effectiveness of mitigation strategies.

Table 4. Effectiveness of Mitigation Strategies.

Mitigation Strategy	Reduction in Frequency	Reduction in Impact
Multi-Factor Authentication	35%	30%
Employee Training	40%	25%
Regular Software Updates	50%	40%
Endpoint Detection Tools	45%	50%

5. Discussion

This discussion analyzes the study's results on cyber assaults, correlating them with current literature and emphasizing their consequences for cybersecurity strategies. It also analyzes the obstacles and prospective trajectories in mitigating cyber risks.

5.1. Analysis of Results

- Frequency and Progression of Cyber Attacks:

The research indicated that hacking is the predominant kind of cyber assault, with its incidence increasing consistently over the last three years. This corresponds with current research that emphasizes the increase of hacking tools and tactics, including brute force assaults and phishing efforts, aimed at the expanding population of digital users and services. The rise in viruses and malware instances indicates the growing attack surface generated by IoT devices and cloud-based systems. The increase in targeted assaults and electronic espionage signifies a transition to more strategic and sophisticated threats, often supported by organized criminal syndicates or state-sponsored entities.

- Economic Consequences:

The economic research verifies that targeted assaults and cyber espionage are the most financially detrimental. These data substantiate the assertion that cybercriminals and adversarial groups are focusing on high-value targets, including firms possessing intellectual property and operators of essential infrastructure. Prior research has shown the cascading consequences of such assaults, including reputational harm and regulatory sanctions, hence exacerbating their financial impact.

- Vulnerabilities inside the Industry:

The sectoral examination of cyber risks underscores the need for tailored cybersecurity policies for each industry. Financial companies must emphasize defenses against hacking, while healthcare providers should concentrate on avoiding malware infections that might interrupt operations. The distinct susceptibility of the technology and military industries to electronic espionage highlights the need of sophisticated encryption and the exchange of threat intelligence to safeguard critical information. These findings align with data indicating that customized strategies provide superior outcomes compared to standard cybersecurity measures.

- *Implementation of Holistic Strategies:*

The efficacy of mitigation techniques, including routine software updates and endpoint detection technologies, highlights the need of implementing a multi-layered cybersecurity system. Organizations

have to amalgamate technology safeguards with staff training initiatives to mitigate both technical and human risks.

- *Focus on Proactive Strategies:*

The consistent increase in targeted assaults and cyber espionage underscores the need for preemptive strategies, including real-time threat information and predictive analytics. These strategies may facilitate the identification of possible hazards before to their emergence, hence mitigating their effect.

- *Stakeholder Collaboration:*

Due to the worldwide and cross-sector characteristics of cyber threats, cooperation among governments, business entities, and cybersecurity professionals is essential. Public-private partnerships and international collaboration may improve resource distribution, information exchange, and the formulation of cohesive cybersecurity policy.

5.3. Challenges in Mitigating Cyber Threats

- Accelerating Threats:

Cyber dangers advance more rapidly than the protections established to combat them. Malefactors harness developing technology, such artificial intelligence and quantum computing, to devise novel exploitation techniques, complicating businesses' ability to adapt.

- Human Factors:

Notwithstanding technological developments, human error continues to be a major factor in cyber events. Phishing and social engineering assaults capitalize on workers' lack of understanding, underscoring the need for ongoing training and awareness initiatives.

- Constraints on Resources:

Small and medium-sized organizations (SMEs) sometimes lack the resources necessary to deploy modern cybersecurity safeguards, leaving them susceptible to assaults. Bridging this gap requires cost-effective solutions and focused assistance from governmental and industrial authorities.

5.4. Prospective Directions

- Investment in Research and Innovation:

Ongoing investment in cybersecurity research is crucial to address the swiftly changing threat environment. Domains include artificial intelligence-enhanced threat detection, blockchain-secured systems, and post-quantum cryptography provide potential for future security measures.

- Strengthening Legal and Policy Frameworks:

As cyber threats become more sophisticated, legal and regulatory frameworks must adapt to confront evolving concerns. Enhancing legislation pertaining to cybercrime, advancing international treaties, and instituting explicit standards for incident reporting and response are essential measures.

- Cultivating a Cyber-Resilient Culture:

Organizations must promote a culture of cybersecurity resilience, ensuring that each person comprehends their responsibility in safeguarding digital assets. This includes consistent training, advocating a zero-trust framework, and securing leadership commitment to cybersecurity. This debate emphasizes the need of completely tackling cyber dangers by contextualizing the results within previous research. Despite substantial advancements in comprehending and alleviating these risks, continuous endeavors are essential to adjust to their changing characteristics and protect vital systems and information.

6. Conclusion

This research analyzed many categories of cyber assaults—hacking, viruses, targeted attacks, and electronic espionage—emphasizing their prevalence, economic repercussions, industrial susceptibilities, and countermeasures. The results highlight the dynamic and intricate nature of cyber threats, necessitating customized, proactive, and cooperative strategies for cybersecurity. Hacking has become the predominant mode of assault, propelled by the growing digitization of services and the accessibility of automated tools. Viruses and malware, while often less advanced, remain substantial dangers to businesses dependent on operational continuity, such as healthcare and manufacturing. Targeted assaults and electronic espionage, albeit seldom, are the most serious categories of cyber risks

for financial and strategic repercussions. These results correspond with the increasing complexity of cybercriminals and state-sponsored entities.

The analysis underscores notable industry-specific vulnerabilities, including banking, healthcare, government, and military as primary targets for various attack modalities. This underscores the need for companies to have tailored cybersecurity policies that mitigate their specific risks. Moreover, the examination of mitigation measures indicated that frequent software upgrades, personnel training, endpoint detection technologies, and multi-factor authentication are critical elements of a comprehensive protection system. The report recognizes several problems, such as the fast progression of cyber threats, the human element in security violations, and budget limitations, especially for smaller entities. Confronting these difficulties requires ongoing innovation, investment in research, and improved coordination among governments, the commercial sector, and cybersecurity professionals. In conclusion, as cyber threats increase in complexity and magnitude, a multi-faceted, adaptable, and cooperative strategy is needed for safeguarding digital security. By merging technology innovations with a robust focus on human awareness and global collaboration, companies and governments may enhance the protection of their systems, data, and stakeholders against the persistent danger of cyber assaults.

Author Contributions: Author has contributed significantly to the development and completion of this article.

Funding: This article received no external funding.

Data Availability Statement: Not applicable.

Acknowledgments: The authors would like to express their sincere gratitude to the Department of Electronics Commerce, Faculty of Economics and Political Science, Bani Waleed University, Libya, for their invaluable support and resources throughout the course of this research.

Conflicts of Interest: The author(s) declare no conflict of interest.

ORCID
Mustafa A. O. Abo Mhara https://orcid.org/0009-0000-0152-5560
Abdullah A. A. Abdulrahman https://orcid.org/0009-0002-7015-2678
Abdulhakim A. S. Baroud https://orcid.org/0009-0004-1006-4697

References

[1] Yaacoub, J.P.A.; Noura, H.N.; Salman, O.; Chehab, A. Robotics cyber security: Vulnerabilities, attacks, countermeasures, and recommendations. Int. J. Inf. Secur. 2021, 21, 115–158.

[2] Taylor, P.J.; Dargahi, T.; Dehghantanha, A.; Parizi, R.M.; Choo, K.-K.R. A systematic literature review of blockchain cyber security. Digit. Commun. Netw. 2020, 6, 147–156.

[3] Kaur, J.; Ramkumar, K.R. The recent trends in cyber security: A review. J. King Saud Univ.-Comput. Inf. Sci. 2022, 34, 5766–5781.

[4] Maglaras, L.A.; Kim, K.-H.; Janicke, H.; Ferrag, M.A.; Rallis, S.; Fragkou, P.; Maglaras, A.; Cruz, T.J. Cyber security of critical infrastructures. ICT Express 2018, 4, 42–45

[5] Waseem, M.; Khan, M.A.; Goudarzi, A.; Fahad, S.; Sajjad, I.A.; Siano, P. Incorporation of Blockchain Technology for Different Smart Grid Applications: Architecture, Prospects, and Challenges. Energies 2023, 16, 820.

[6] Khan, M.A.; Saleh, A.M.; Waseem, M.; Sajjad, I.A. Artificial Intelligence Enabled Demand Response: Prospects and Challenges in Smart Grid Environment. IEEE Access 2023, 11, 1477–1505.

[7] Aslan, O.; Yilmaz, A.A. A New Malware Classification Framework Based on Deep Learning Algorithms. IEEE Access 2021, 9, 87936–87951.

[8] Aslan, O.; Ozkan-Okay, M.; Gupta, D. Intelligent Behavior-Based Malware Detection System on Cloud Computing Environment. IEEE Access 2021, 9, 83252–83271.

[9] Paolini, A.; Scardaci, D.; Liampotis, N.; Spinoso, V.; Grenier, B.; Chen, Y. Authentication, Authorization, and Accounting. Towards Interoper. Res. Infrastruct. Environ. Earth Sci. 2020, 12003, 247–271.

[10] Javaheri, D.; Hosseinzadeh, M.; Rahmani, A.M. Detection and Elimination of Spyware and Ransomware by Intercepting Kernel-Level System Routines. IEEE Access 2018, 6, 78321–78332.

[11] Clausen, H.; Grov, G.; Sabate, M.; Aspinall, D. Better Anomaly Detection for Access Attacks Using Deep Bidirectional LSTMs. In Proceedings of the International Conference on Machine Learning for Networking, Paris, France, 24–26 November 2020; pp. 1–18.

[12] Humayun, M.; Niazi, M.; Jhanjhi, N.; Alshayeb, M.; Mahmood, S. Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. Arab. J. Sci. Eng. 2020, 45, 3171–3189.

[13] Tundis, A.; Mazurczyk, W.; Mühlhäuser, M. A review of network vulnerabilities scanning tools: Types, capabilities and functioning. In Proceedings of the 13th International Conference on Availability, Reliability and Security, Hamburg, Germany, 27–30 August 2018; pp. 1–10.

[14] Joshi, C.; Singh, U.K. Security testing and assessment of vulnerability scanners in quest of current information security landscape. Int. J. Comput. Appl. 2016, 145, 1–7.

[15] Wang, Y.; Yang, J. Ethical hacking and network defense: Choose your best network vulnerability scanning tool. In Proceedings of the 2017 31st International Conference on Advanced Information Networking and Applications Workshops, Taipei, Taiwan, 27–29 March 2017; pp. 110–113.