STM JOURNALS

International Journal of
Information Security Engineering

ISSN: 3049-1150
Volume 3, Issue 2, 2025
July–December
DOI (Journal): 10.37591/IJISE

https://journals.stmjournals.com/ijise

Research IJISE

An In-depth Analysis of Cyberattacks and Cybersecurity: New Trends and Advancements

Deepak Kumar Sharma[1,*], Tejinder Pal Singh Brar[2]

Abstract

At present, a significant portion of global economic, commercial, cultural, social, and governmental activities and interactions, including those involving individuals, NGOs, and state institutions, takes place in cyberspace. In recent times, many businesses and government agencies around the world have been facing the growing challenge of cyberattacks and the risks associated with wireless communication technologies. As modern society becomes increasingly dependent on digital technologies, protecting sensitive information from cyber threats has become a major concern. The primary aim of cyberattacks is often to cause financial harm to organizations, although in some cases, they may also pursue military or political objectives. This study aims to explore and critically assess the current developments in the field of cybersecurity, while also identifying the challenges, weaknesses, and advantages of the proposed approaches. A variety of novel descendant assaults are examined in depth. Standard security frameworks are examined alongside the historical context and early-generation cybersecurity methodologies. Additionally, developing trends and current breakthroughs in cybersecurity, along with associated dangers and difficulties, are addressed. The thorough review study given for IT and cybersecurity researchers is anticipated to be beneficial.

Keywords: Security, cyber security, threats, cybercrime, cyber warfare

INTRODUCTION

For over 20 years, the Internet has significantly influenced global communication and has become increasingly embedded in the lives of individuals worldwide. Innovations and cost reductions in this domain have markedly enhanced the accessibility, utilization, and efficacy of the Internet, resulting in around 3 billion users globally today [1].

The Internet has established an extensive worldwide network that generates billions of dollars each year for the global economy [2]. Today, most economic, commercial, cultural, social, and governmental interactions between countries, including those involving individuals, NGOs, and state institutions, take place within cyberspace. Critical and sensitive infrastructures and systems either constitute a component of cyberspace or are governed, administered, and utilized through this domain, with the majority of essential and sensitive information being transmitted to this area. This has been established in this domain [3]. A substantial portion of the material and spiritual capital of nations is allocated to this domain, and a considerable share of people' material wealth and spiritual accomplishments is derived from or significantly influenced by this space [4]. In other words, several facets of people' life are intrinsically

***Author for Correspondence**
Deepak Kumar Sharma
E-mail: dksharma100898@gmail.com

[1]Research Scholar, Department of Computer Technology, M.M. Institute of Computer Technology & Business Management, Maharishi Markandeshwar (Deemed to be University), Mullana, Ambala, Haryana, India
[2]Professor, Department of Computer Technology, M.M. Institute of Computer Technology & Business Management, Maharishi Markandeshwar (Deemed to be University), Mullana, Ambala, Haryana, India

Received Date: April 22, 2025
Accepted Date: June 19, 2025
Published Date: July 24, 2025

Citation: Deepak Kumar Sharma, Tejinder Pal Singh Brar. An In-depth Analysis of Cyberattacks and Cybersecurity: New Trends and Advancements. International Journal of Information Security Engineering. 2025; 3(2): 31–38p.

connected to this space, and any instability, insecurity, or obstacles inside it will immediately impact these facets [5]. Nonetheless, cyberspace has presented novel security issues to nations. For almost 10 years, experts have contemplated the potential ramifications of cyberattacks [6–8]. This research initially elucidates the nature of cyberattacks, subsequently examines their categorization and classification, and lastly investigates and analyzes current definitions from the perspectives of worldwide specialists and organizations. The conclusion of the study is delivered finally.

FUNDAMENTAL CONCEPTS

Cyberattacks cover a broader range of activities than those typically included under the term information operations. Information operations entail the coordinated use of primary electronic warfare capabilities, psychological tactics, computer network strategies, military deception, and security operations, alongside specialized support and pertinent skills, to influence, disrupt, eliminate, or commandeer human decision-making processes. This constitutes a decision-making process of national institutions. Figure 1 presents the structure of a cyberattack. According to the USNM Strategy for cyberspace operations, computer network operations include offensive actions, defensive measures, and support functions. Unlike direct attacks or defensive strategies, this type of operation focuses primarily on gathering and analyzing information rather than interfering with network functionality, and it can act as a preliminary step to a cyberattack [9]. Such operations may also be used for spreading information or propaganda. Additionally, computer networks can be exploited to obtain essential data from targeted systems [10].

Furthermore, five situations may be contemplated about cyber warfare: (1) State-sponsored cyber espionage to acquire intelligence for future cyber offensives, (2) a cyber assault designed to instigate unrest and civil insurrection, (3) a cyber offensive intended to incapacitate infrastructure and enable physical hostilities, (4) cyber operations serving as an adjunct to conventional military aggression, and (5) cyberattacks aimed at achieving extensive devastation or disruption as the primary objective (cyber warfare) [11].

A form of cyberattack is encryption. Encryption is a reversible technique for encoding data that necessitates a key for decryption. Encryption can be utilized with encryption, offering an additional layer of secrecy. Encryption involves the application and analysis of data encoding and decoding, ensuring that only designated personnel may access the decrypted information. The mechanism for encrypting and decrypting data is the encryption system [12]. It is essential to understand that cybercrime, cyberwarfare, and cyberattacks are distinct concepts. Figure 2 and Table 1 illustrate and clarify the conceptual differences between these three forms of cyber activity.

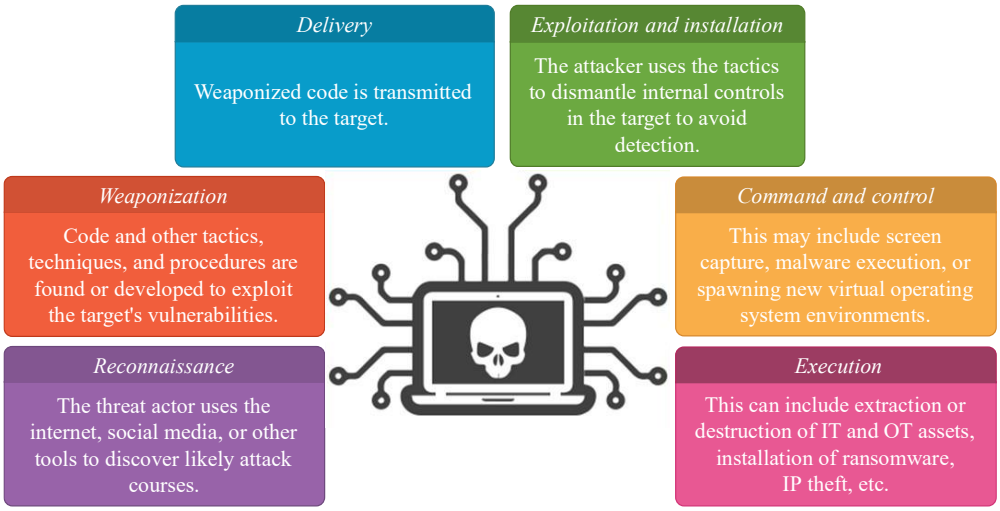

Figure 1. Anatomy of a cyberattack.

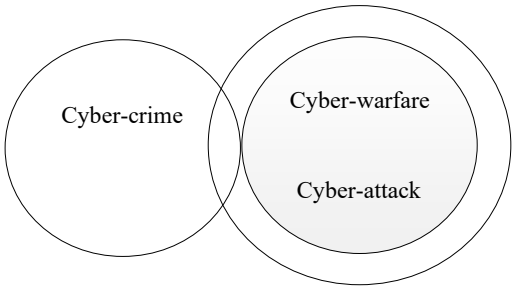

Figure 2. Distinction between cyber-crime, cyber-warfare, and cyber-attack.

Table 1. Distinction between cyber-crime, cyber-attacks, and cyber-warfare.

Type of cyber action	Nature and characteristics
Cyber-crime	Cyber actions taken only by non-governmental attackers.
Cyber-crime	The cyber action is carried out by a computer system and is merely in violation of criminal law
Cyber-attack and cyber-warfare	The purpose of a cyber-attack is to destroy and disrupt the operation of a computer network
Cyber-attack and cyber-warfare	The attack must have political or security purposes.
Cyber-warfare	The effects of a cyber-attack are the same as an armed attack or the cyber act took place in the context of an armed attack.

Definition of Cyber-attack from the Perspective of Specialists

Numerous definitions of cyberattack have been formulated by experts in both legal and technological domains, the most significant of which are as follows:

1. *Richard Clark* defines cyberattacks as activities executed by nations to penetrate the computer systems or networks of another country, aiming to inflict harm or disruption. The examination and critique of this definition indicate that the three elements, namely, the assailant, the objective, and the aim of the attack, have been employed as criteria, neglecting the forms of disruption [13]. Furthermore, about the assailant of the attack, only nations are referenced broadly; nevertheless, if an assault occurs inside the context and geographical domain governed by a nation (the cyberspace of networks under national control) by persons; and if non-governmental and private entities engage in actions against a third nation, they will essentially be excluded from the aforementioned criteria, resulting in a legal void regarding such assaults. In light of this condition, it can be asserted that the aforementioned definition is predominantly inadequate and omits a substantial portion of the assaults executed by private and non-governmental entities, resulting in a deficiency [14].
2. *Michael Hayden:* Any deliberate effort to interfere with or obliterate another nation's computer networks [15]. In contrast to the initial definition, which confined the assailants of the attack to state actors, this broader definition is easily interpretable and, as noted, may pose risks, yield adverse consequences, and engender confusion in international relations, ultimately threatening global peace [16].
3. *Martin Libicki:* Digital assaults on computer systems render them seemingly normal while generating and disseminating false replies. This method of classifying cyberattacks effectively omits several potential risks to the national security of a nation whose cyber infrastructure has been compromised but has not attained the threshold of significant assaults. These threats have the potential to damage the computer networks and systems of the nation being targeted. Consequently, any definition of a cyberattack that omits the aforementioned elements would be inherently inadequate and lack the requisite comprehensiveness [17].
4. *Group of the Tallinn Manual:* A cyberattack is a cyber activity, either offensive or defensive, that may result in injury or death to individuals or inflict damage or destruction to property. The ambiguity of this concept lies in the outcomes and consequences achieved. According to the definition's suppliers, a cyberattack qualifies as an attack if it results in the specified outcomes, namely personal and financial harm [18].

CYBERSECURITY THREATS

The global cyberspace inherently generates overlapping domains of control for national entities, each possessing distinct legal, cultural frameworks and strategic interests [19]. Countries globally have become more reliant on cyberspace for communication and the management of the physical realm, rendering separation from it unequivocally impossible. Consequently, the security responsibilities and operations of each nation are increasingly influenced by cyberspace [20]. The worldwide manufacturing of software and hardware makes it impossible to fully secure the product supply chain. The scalability of the cyber domain renders it qualitatively distinct. A bomb possesses a restricted physical range under the most severe conditions; conversely, cyber threats exhibit an extensive range of impacts, so we have a system capable of regulating real-world activities. As in many other fields, a small group of individuals holds control over activities in cyberspace. Most users are unable to modify or control the software and hardware they use. Only a select few possess the expertise to effectively manage or conduct cyber warfare as shown in Figure 3 [21].

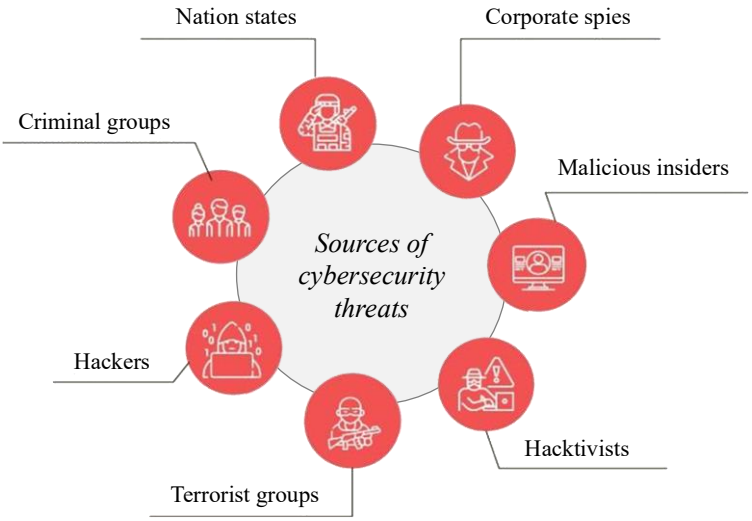

Figure 3. Depicts the sources of cyber dangers.

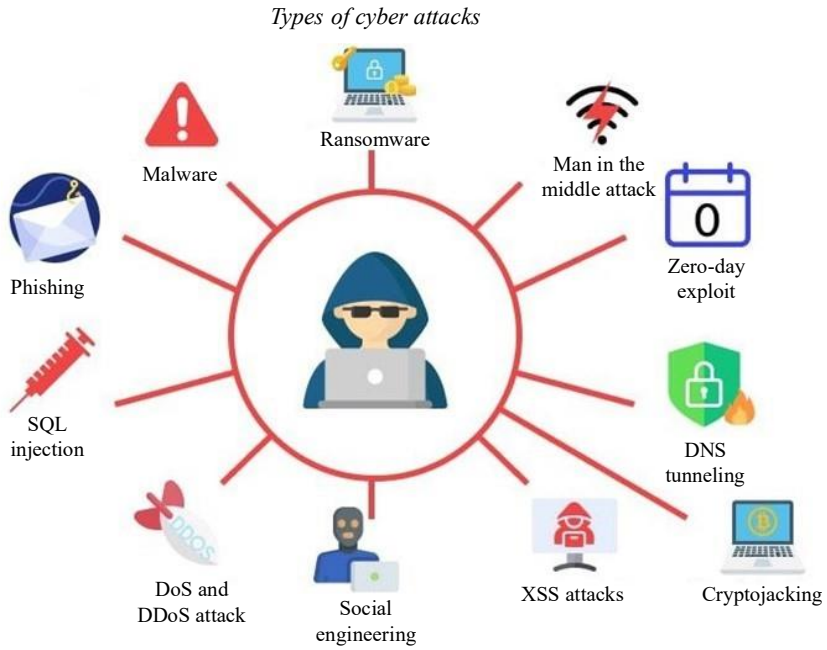

Figure 4. Main cyberattack types.

Key cyberattack strategies include Denial of Service (DoS), logic bombs, misuse of tools, sniffers, Trojan horses, viruses, worms, spam distribution, and botnets. Figure 4 illustrates the primary types of cyber threats. The Denial of Service technique disrupts system availability, preventing legitimate users from accessing the system and potentially allowing unauthorized access instead. The assailant, from a singular point, initiates an inundation of communications to the target systems, therefore obstructing the legitimate flow of data. This inhibits any system from utilizing the Internet or engaging in communication with other systems. In an alternative approach known as pervasive Denial of Service, the assault is executed from several dispersed systems concurrently rather than from a singular source. This is frequently accomplished by deploying worms and replicating them across several computers to assault the target. Publicly accessible abuse tools exist that may identify and exploit vulnerabilities in networks across various skill levels [22].

A logic bomb is a type of cyberattack in which a programmer inserts malicious code into a program, designed to automatically execute harmful actions when a specific condition or event takes place [23–25]. The implications and risks of cybersecurity in WAMS-based FFR (Fractional Flow Reserve) regulation were examined using an innovative scale CNN for the analysis of spoofing data over two scales. The time-frequency-based cybersecurity defensive strategy for the FFR system was also evaluated, focusing on its effectiveness in detecting and mitigating cyber-attacks in real-time [26].

CYBERSECURITY

Cybersecurity is a vital aspect of the infrastructure within any company or organization. In summary, a cyber security firm or organization may attain significant prestige and numerous achievements, since this success stems from its capacity to safeguard private and client data from competitors. Organizations and rivals of clients and people exhibit abusive behavior as shown in Figure 5.

Network security safeguards the computer network against disruptors, including virus and hacker attempts. Network security comprises a collection of measures that allow enterprises to protect computer networks against hackers, coordinated attacks, and viruses [27].

- *Application security:* Utilizing both hardware and software, such as firewalls, encryption tools, and antivirus programs, protects the system against external threats that could interfere with the development of applications.
- *Information security:* Safeguards physical and digital data from illegal access, disclosure, abuse, alterations, and destruction.
- *Operational security:* Encompasses procedures and determinations used to manage and safeguard data. For instance, user rights for network access or protocols that dictate the conditions under which information may be kept or disseminated.
- *Cloud security:* Safeguards data on the cloud (dependent on the software) and oversees the mitigation of on-site attack threats.
- *User instruction:* Denotes the unexpected elements of cybersecurity, namely persons. Anyone may inadvertently introduce a virus into the security system. Instructing users to eliminate dubious email attachments, refrain from connecting to unidentified USB devices, and address other vital concerns must be integral to every organization's corporate security strategy, as these techniques are frequently employed by cybercriminals. The security of an organization is founded on three principles: secrecy, integrity, and availability. These three core principles, commonly referred to as the CIA triad or security triangle, have served as the foundation for system security since the early days of computing (Figure 5) [28]. The concept of secrecy asserts that only authorized entities may access sensitive information and operations, such as classified military information (Confidentiality). The principles of integrity assert that only authorized personnel and resources are permitted to edit, add, or delete sensitive information and functions; such as a user inputs erroneous data into a database (Integrity). Availability principles assert that systems, services, and data must be accessible on demand according to predetermined criteria established by the Service Level Agreement (SLA).

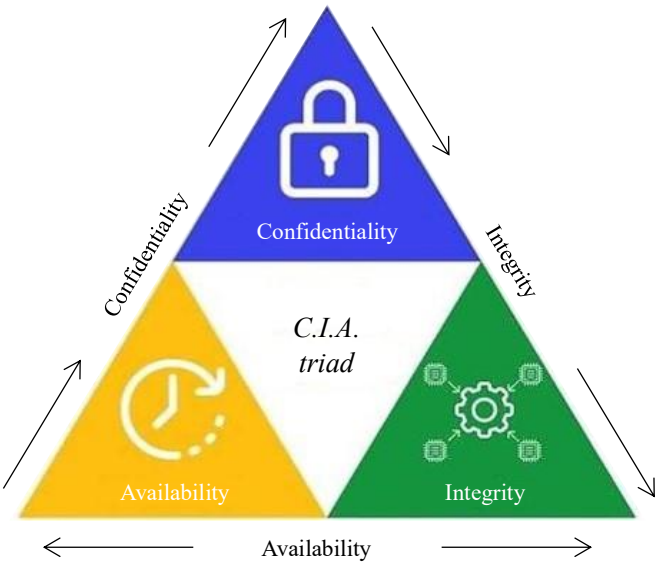

Figure 5. Security triangle (CIA)

Application security begins with superior encryption: Each plan must be uniquely tailored and executed for each organization. This method reduces the occurrence of information hacking and infiltration. Cyber security is growing progressively intricate. Organizations must adopt a "security perspective" about the functioning of cyber-security. As a result, it is essential to uphold strong security protocols to outpace cybercriminals. As security concerns escalate, investment in cyber security systems and services is increasing. The three businesses operating in this sector are McAfee, Cisco, and Trend Micro [29–31].

Cyber-security Policy

Cyber has enhanced the community's productivity and efficiently disseminated knowledge throughout time. Regardless of the application or sector in which cybersecurity is employed, the enhancement of production has consistently been a priority. Rapid data transmission to cyberspace predominantly diminishes overall system security. Technology professionals enhancing production frequently encounter a dichotomy between security indicators and progress, as preventive measures can restrict, hinder, or postpone user access, while consumption indicators highlight essential system resources and attract managerial focus. Cyber security policy may stipulate that when the danger of disclosing sensitive information is elevated, information should not be sent without a thorough assessment of the recipient's capacity to uphold information security [32, 33].

CONCLUSION

In the third millennium, cyberspace and related technologies have become major sources of power. Due to features like low entry barriers, anonymity, vulnerability, and asymmetry, power is becoming more dispersed. This means that although governments have traditionally held centralized control, other actors, such as private companies, criminal and terrorist groups, and even individuals, are gaining significant influence. Nonetheless, governments still remain important players in this evolving landscape. This occurrence will not compromise national security for countries. This impact may be assessed using many methods.

- The *first* notion is security. National security can no longer be characterized solely by military concerns and territorial boundaries; rather, the deterioration of people' quality of life now constitutes a significant danger to national security.
- The *second* aspect is the vanishing of the geographical component of cyber threats. Historically, military dangers were associated with distinct geographical locations. Consequently, it was quite straightforward to manage, particularly regarding identification.

- The *third* factor is the magnitude of vulnerabilities presented by cyberattacks. These dangers are intermittent, multifaceted, and because to their connection with critical networks and infrastructure, their potential for harm is substantial.
- *Fourth*, these threats cannot be mitigated solely through conventional methods, such as military and police force; governments alone are inadequate to address them. Effective bilateral cooperation between governments and the private sector, which shares common interests in addressing these threats, is essential.
- *Fifth*, as the preceding point indicates, cyber risks extend beyond governments; people and corporations are also susceptible to the detrimental effects of these threats.
- *Sixth*, as security in the digital age transcends political boundaries, the many theoretical frameworks in international relations, predominantly grounded in governmental paradigms, are often disregarded or rendered ambiguous.

REFERENCES

1. Aghajani G, Ghadimi N. Multi-objective energy management in a micro-grid. Energy Rep. 2018 Nov 1; 4: 218–25.
2. Akhavan-Hejazi H, Mohsenian-Rad H. Power systems big data analytics: An assessment of paradigm shift barriers and prospects. Energy Rep. 2018 Nov 1; 4: 91–100.
3. Al Shaer D, Al Musaimi O, de la Torre BG, Albericio F. Hydroxamate siderophores: Natural occurrence, chemical synthesis, iron binding affinity and use as Trojan horses against pathogens. Eur J Med Chem. 2020 Dec 15; 208: 112791.
4. Alkatheiri MS, Chauhdary SH, Alqarni MA. Seamless security apprise method for improving the reliability of sustainable energy-based smart home applications. Sustain Energy Technol Assess. 2021 Jun 1; 45: 101219.
5. Alzubaidi A. Cybercrime awareness among Saudi nationals: dataset. Data Br. 2021 Jun 1; 36: 106965.
6. Baig ZA, Szewczyk P, Valli C, Rabadia P, Hannay P, Chernyshev M, Johnstone M, Kerai P, Ibrahim A, Sansurooah K, Syed N. Future challenges for smart cities: Cyber-security and digital forensics. Digit Investig. 2017 Sep 1; 22: 3–13.
7. Beechey M, Kyriakopoulos KG, Lambotharan S. Evidential classification and feature selection for cyber-threat hunting. Knowl-Based Syst. 2021 Aug 17; 226: 107120.
8. Brar TP. Secure E-Banking Environment: A Comparative Analysis of Various Security Aspects. International Journal of Emerging Issues in Management and Technology (IJEIMT). 2016; 1(3): 22–30.
9. Bullock JA, Haddow GD, Coppola DP. Cybersecurity and critical infrastructure protection. In: Bullock JA, Haddow GD, Coppola DP, editors. Introduction to Homeland Security. 6th ed. Amsterdam: Butterworth-Heinemann; 2021. p. 425–97. doi: 10.1016/B978-0-12-817137-0.00008-0.
10. Cao J, Ding D, Liu J, Tian E, Hu S, Xie X. Hybrid-triggered-based security controller design for networked control system under multiple cyberattacks. Inf Sci. 2021 Feb 16; 548: 69–84.
11. Chandra A, Snowe MJ. A taxonomy of cybercrime: Theory and design. Int J Account Inf Syst. 2020 Sep 1; 38: 100467.
12. Chen JK, Chang CW, Wang Z, Wang LC, Wei HS. Cyber deviance among adolescents in Taiwan: Prevalence and correlates. Child Youth Serv Rev. 2021 Jul 1; 126: 106042.
13. Cheng S, Zhao G, Gao M, Shi Y, Huang M, Marefati M. A new hybrid solar photovoltaic / phosphoric acid fuel cell and energy storage system; Energy and Exergy performance. Int J Hydrog Energy. 2021 Feb 11; 46(11): 8048–66.
14. Edgar TW, Manz DO. Science and cyber security. In: Edgar TW, Manz DO, editors. Research Methods for Cyber Security. Amsterdam: Syngress; 2017. p. 33–62. doi: 10.1016/B978-0-12-805349-2.00002-9.
15. Furnell S, Shah JN. Home working and cyber security–an outbreak of unpreparedness? Comput Fraud Secur. 2020 Aug 1; 2020(8): 6–12.
16. Gandhi P, Sharma RK, Brar TPS, Bhatia P. Significance of data mining in the domain of intrusion detection. In: Gandhi P, Bhatia S, Dev K, editors. Data Driven Decision Making Using Analytics. Boca Raton: CRC Press; 2021. p. 16. doi: 10.1201/9781003199403.

17. Hart S, Margheri A, Paci F, Sassone V. Riskio: A serious game for cyber security awareness and education. Comput Secur. 2020 Aug 1; 95: 101827.
18. Huang J, Ho DW, Li F, Yang W, Tang Y. Secure remote state estimation against linear man-in-the-middle attacks using watermarking. Automatica. 2020 Nov 1; 121: 109182.
19. Iqbal Z, Anwar Z. SCERM—A novel framework for automated management of cyber threat response activities. Future Gener Comput Syst. 2020 Jul 1; 108: 687–708.
20. Yang SH, Cao Y, Wang Y, Zhou C, Yue L, Zhang Y. Harmonizing safety and security risk analysis and prevention in cyber-physical systems. Process Saf Environ Prot. 2021 Apr 1; 148: 1279–91.
21. Khan SK, Shiwakoti N, Stasinopoulos P, Chen Y. Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions. Accid Anal Prev. 2020 Dec 1; 148: 105837.
22. Kharlamova N, Hashemi S, Træholt C. Data-driven approaches for cyber defense of battery energy storage systems. Energy AI. 2021 Sep 1; 5: 100095.
23. Lee C, Chae YH, Seong PH. Development of a method for estimating security state: Supporting integrated response to cyber-attacks in NPPs. Ann Nucl Energy. 2021 Aug 1; 158: 108287.
24. Li J, Sun C, Su Q. Analysis of cascading failures of power cyber-physical systems considering false data injection attacks. Glob Energy Interconnect. 2021 Apr 1; 4(2): 204–13.
25. Li N, Tsigkanos C, Jin Z, Hu Z, Ghezzi C. Early validation of cyber–physical space systems via multi-concerns integration. J Syst Softw. 2020 Dec 1; 170: 110742.
26. Liu X, Zhang J, Zhu P, Tan Q, Yin W. Quantitative cyber-physical security analysis methodology for industrial control systems based on incomplete information Bayesian game. Comput Secur. 2021 Mar 1; 102: 102138.
27. Mehrpooya M, Ghadimi N, Marefati M, Ghorbanian SA. Numerical investigation of a new combined energy system includes parabolic dish solar collector, Stirling engine and thermoelectric device. Int J Energy Res. 2021 Sep; 45(11): 16436–55.
28. Le Nguyen C, Golman W. Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries: 'Law on the books' vs 'law in action'. Comput Law Secur Rev. 2021 Apr 1; 40: 105521.
29. Ogbanufe O. Enhancing end-user roles in information security: Exploring the setting, situation, and identity. Comput Secur. 2021 Sep 1; 108: 102340.
30. Patel DC, Berry MF, Bhandari P, Backhus LM, Raees S, Trope W, Nash A, Lui NS, Liou DZ, Shrager JB. Paradoxical motion on sniff test predicts greater improvement following diaphragm plication. Ann Thorac Surg. 2021 Jun 1; 111(6): 1820–6.
31. Priyadarshini I, Kumar R, Sharma R, Singh PK, Satapathy SC. Identifying cyber insecurities in trustworthy space and energy sector for smart grids. Comput Electr Eng. 2021 Jul 1; 93: 107204.
32. Qiu W, Sun K, Yao W, You S, Yin H, Ma X, Liu Y. Time-frequency based cyber security defense of wide-area control system for fast frequency reserve. Int J Electr Power Energy Syst. 2021 Nov 1; 132: 107151.
33. Tam T, Rao A, Hall J. The good, the bad and the missing: A Narrative review of cyber-security implications for Australian small businesses. Comput Secur. 2021 Oct 1; 109: 102385.

