www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 04, Issue 10, October 2024, pp : 673-679

e-ISSN : 2583-1062
Impact Factor : 7.001

AN ANALYSIS OF CYBER SECURITY INCLUDING NEW ADVANCEMENTS AND EMERGING TRENDS

Aishwarya Gupta[1]

[1]Dr. Preeti Global University, Dinara, M.P., India.

Email: guptaaishwarya006@gmail.com

DOI: https://www.doi.org/10.58257/IJPREMS36301

ABSTRACT

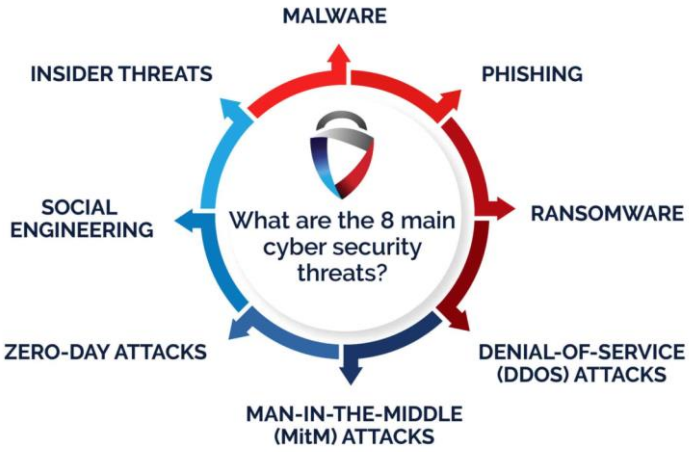
These days, the majority of international relations, economic, commercial, cultural, social, and governmental interactions occur online between nations at all levels, including people, non-governmental organizations, and governments and government agencies. The issue of cyber attacks and the risk posed by "wireless communication technology" have recently become global concerns for several government agencies and commercial businesses. Modern society is heavily reliant on electronic technology, making it difficult to safeguard this data against cyber attacks. Cyber attacks are intended to cause financial harm to businesses. Cyber attacks may serve military or political objectives in certain other situations. DDS "Data distribution services", computer viruses, knowledge gaps, and other attack vectors are a few examples of these harms. In order to mitigate the harm caused by cyber attacks, different organizations employ different strategies. Cyber security stays up to date with the most recent IT data. To date, several approaches have been put forth by researchers worldwide to either stop cyber attacks or lessen the harm they do. There are methods in the working phase and methods in the "study phase". The purpose of this work is to examine the advantages, disadvantages, and strengths of the suggested approaches while surveying and deeply reviewing the typical modifications made in the field of "cyber security". A detailed consideration of many new descendant assault kinds is given. The history of "early-generation cyber-security techniques" and standard security frameworks are examined. Furthermore, new advancements, emerging trends, and security concerns and issues related to cyber security are discussed.

1. INTRODUCTION

Over the "course of two decades", the Internet has rises in "importance and permeated" people's lives all over the world, playing a critical role in international communication. The Internet is being used by around 3 billion people globally thanks to advancements in affordability and usability that have greatly improved its availability, functionality, and performance (Tan et al., 2021).A huge worldwide network that the "Internet has produced" has brought "billions of dollars" to the world economy every year (Judge et al., 2021). Most international contacts and activities related to trade, politics, culture, economy, and non-governmental organizations now take place mostly online "Aghajani and Ghadimi, 2018". This includes interactions between people, non-governmental organizations, and government and governmental institutions. The majority of the sensitive and important data is either transported to or essentially produced in cyberspace and vital and sensitive infrastructures and systems constitute a component of cyberspace itself or are controlled, managed, and exploited through this space "Akhavan-Hejazi and Mohsenian-Rad, 2018". The leadership of "media activities" are moved into this area, the "majority of financial transactions" take place there, and a sizeable portion of residents' free time and activities are spent engaging there (Priyadarshini et al., 2021). The GDP of nations now includes a far larger portion of revenue from cyber businesses, and among the metrics used to gauge the level of growth, cyberspace indicators play a key role. A considerable portion of a nation's material and spiritual capital is found in this area, and a sizable portion of its inhabitants' material income and spiritual accomplishments are either gained in this area or significantly influence it (Amir and Givargis, 2020). Put another way, many facets of citizens' lives are inextricably linked to this area, and any instability, insecurity, or problems there will have a direct impact on various facets of residents' lives (Lietal., 2020).However, governments now face "additional security" issues as a result of cyberspace. Threats such as cyber warfare, cybercrime, cyber terrorism, and cyber espionage have been brought about by low entry costs, anonymity, and uncertainty of the threatening geographical area, dramatic impact, and lack of public transparency in cyberspace. Strong and weak actors in this space include governments, organized and terrorist groups, and even individuals. Cyber threats are distinct from traditional national security threats, which are characterized by their transparency and the involvement of identifiable governments and nations in a particular region. As a result, national security in its conventional sense is facing difficulties and becoming less effective in this domain (Sarker, 2021). Experts have contemplated the potential ramifications of cyber attacks for almost ten years (Shinetal., 2021).Severe and occasionally widespread physical or economic damage can occur from a variety of scenarios, such as a virus that targets financial records of an economy or interferes with the stock market; it can also cause a country's power plant to malfunction or stop; it can even cause air traffic accidents by interfering with the air "traffic control

system" "Snehi and Bhandari,2021; Ahmed Ja-mal et al., 2021". It will thus be very challenging for professionals to handle the many and varied facets of the problem and offer legal guidance and analysis unless governments develop a clear definition of cyber attack that is approved and welcomed by the international community (Cao et al., 2021). Because of this, the topic of what constitutes a cyber attack, what its attributes are, and whether or not an attack that occurs mostly online qualifies as one in the conventional sense Bholet et al. (2021). It is obvious that the legal environment to continue and identify the effects of this attack type would be directly impacted by the availability of a "thorough definition of a cyber attack" (Furnelletal., 2020).Without a doubt, the absence of a thorough and precise definition results in uncertainty regarding the main legal route, variation in practice and interpretation, and eventually, conflicting legal judgments (Alhayani et al., 2021). Therefore, it is imperative that a thorough research be conducted and that an appropriate definition is established.

Cyberspace threats- Naturally, "national actors with varying legal" and cultural approaches as well as "distinct strategic goals" establish overlapping and overlapping domains of control due to the global cyberspace's reach (Iqbal and Anwar, 2020).It is now difficult to live apart from cyberspace as nations all over the world rely so much on it for control and communication with one another and with the actual world. Thus, cyber security activities and functions are progressively impacted by cyberspace in every nation (Zhao et al., 2020).In the product supply chain process, assurances are not feasible due to the worldwide manufacturing of hardware and software. The cyber domain is distinct due of its scalability. In the most severe circumstances, a bomb's physical range is restricted; but, because cyber threats have a wide range of consequences, we have a system in place to manage real-world activities. Operations in cyberspace are governed by a limited number of people, just like in many other fields of knowledge. The software and hardware that users utilise cannot be changed or altered by them. It's no secret that a select few individuals are capable of efficiently leading or overseeing cyber warfare (Zhang et al., 2021). A single or group of people cannot seek total control in the cyber realm due to its scattered nature, even with the necessary focus and specialised knowledge.



The fast advancement of computing and communication technologies is the driving force behind changes in the realm of cyber. This accelerates when there is cyber cohesiveness. A new period of vulnerability and responsiveness is ushered in by every transition. According to Varga et al. (2021) cyberspace is essentially dynamic and far from static. Cyber assets are dispersed across a wide range of organizations, from closed, government-controlled systems to those owned and operated by the private sector of the economy. Each of these systems has its own unique facilities, capacities, and concerns, and they are all affected differently (Zhao et al., 2021).The nature of cyberspace makes it impossible to confidently attribute actions to specific people, groups, or organizations at this time due to technical limitations.

As per Al-Ghamdi (2021) the principal dangers in cyberspace are: external, "internal supply chain", and risks resulting from inadequate operational capacity of local forces. For part of their intelligence collecting and espionage operations, foreign intelligence agencies employ cyber technologies. A great deal of information infrastructure destruction and abuse, including the abuse of 'computer systems', "Internet information networks", and "processors and controllers" integrated into critical sectors, "has been documented" in several situations throughout the world. According to Beecheyet al. (2021) there is a growing number of groups of persons that attack cyber systems with the intention of making money. To express them, other organizations (hackers) occasionally access the network. These organizations typically put more strain on email servers, and through website hacking, they reveal their political statements (Solomon, 2017).However, the primary source of cybercrime is internal disgruntled agents working within the organization. These agents don't necessarily need to be well-versed in cyber attacks because their target system awareness typically grants them unrestricted access to target systems or steal information from the organization. Another source of threat is

terrorism, which aims to damage, disable, or deliberately use essential infrastructure to jeopardize national security, cause significant losses, impair the nation's economy, and erode public confidence (Saxena and Gayathri, 2021).

Worms and multiplicities computers are frequently used in this way to assault the target. There are public abuse tools that can find and access vulnerabilities in networks with varying levels of expertise. “Li et al. (2021)” and “Marefati et al. (2018)” describe a logic bomb as an additional sort of attack wherein a ‘programmer inserts’ code into a programmed that, upon the occurrence of a certain event, causes the programmed to behave destructively. According to ‘Patel et al. (2021)’ Sniffer is additional software that intercepts data that has been routed and searches each packet in the data stream for definite data, such passwords. As per the Al ‘Shaer et al. (2020)’, a Trojan horse is a unique use that masquerades as a ‘useful program’ that the user is ready to run. Additionally, a virus can corrupt system files by injecting a duplicate of it into those files, which are popular programs. These versions execute and let the virus infect further files by loading compromised data into memory. Viral infections, in contrast to worms, are spread by humans.

By using a unique scale CNN to interpret spoofing data from two scales, Qiu et al. (2021) examined the effects and risks of cyber security in WAMS-based FFR (Fractional Flow Reserve) regulation. They looked at the cyber-security defense architecture for the FFR system that is based on time-frequency analysis as well. In comparison to real synchrophasor data, the outcome demonstrated improved accuracy and robustness. A knowledge-based hidden Makrove modelling was used by Lee et al. (2021) to build a strategy for unified cyber-attack respond process. A security state approximation technique using updated HMMs was also investigated. Conducting a case study has proved the validity of the established strategy. An ideal security portfolio to fend against multistage cyber attacks may be chosen with the help of Zhang and Malacaria's cyber security decision support system (2021).The system was supported by an LM to identify active assaults and included preventative as well as online optimizations.

They find that selecting the suitable answers on the internet was a Bayesian STACKELBERG game. Kimetal (2020) looked studied the factors that might lead to a cyber attack on NPPs. Furthermore, utilising AHP and FA, the comparative importance of the NPP potential factors was quantified. They discovered that the adoption of the “Korean cyber security” strategy was the more preferred course of action. Tosun (2021) demonstrated how cyber attacks exhibit abrupt, negative shocks to a ‘company's popularity’. Financial markets also react to company security lapses by depressing returns further. Additionally, the selling pressure and improved liquidity caused the trading rate to rise. “Long-term R&D” and ‘dividends decline’ while target companies continue to pay their CEOs.

Cyber security- An essential component of every company's or organization's infrastructure is cyber security. To put it succinctly, an organization or corporation founded on cyber security can attain great success and prominence as these accomplishments stem from the organization’s capacity to defend client and private information against rivals. Abuse occurs from companies and rivals who target customers and people. A business or organization must first and foremost offer this security in the most effective manner possible in order to grow and establish itself (Rodríguez- deArriba et al., 2021). Cyber security refers to the actual steps taken to safeguard data, networks, and information from both internal and external threats. Computer systems, servers, intranets, and networks are safeguarded by cyber security professionals. According to Ahmed Jamal et al. (2021) only those with permission may access the data thanks to cyber security measures. Knowing the different kinds of cyber security is essential for effective defense. Various forms of cyber security are illustrated in Fig. 5.Network security guards against malicious software and hacking attempts that may impair the computer network. Organizations may keep computer networks safe from viruses, organized crime, and hackers by using a set of measures known as network security (Zhang, 2021).

Application Security: The system is shielded from outside dangers that might impede the development of applications by using hardware and software (firewalls, encryption, and anti-virus programs) (Alkatheiri et al., 2021).

The decisions and procedures used to manage and safeguard data are referred to as operational security. One instance of this would be user rights for network access or procedures that dictate the locations and times at which data may be exchanged or stored (Ogbanufe, 2021).

According to Krishnasamy and Venkatachalam (2021) cloud security guards data stored in the cloud using software and keeps an eye out for any on-site threats.

User training: Discusses the unpredictable (i.e., personal) aspects of cyber security. An inadvertent virus infection of the security system might happen to anybody. A corporate security plan for each organization should include instruction on how to handle suspicious email attachments, avoid connecting to anonymous USBs, and handle other important difficulties (Krishnasamy and Venkatachalam, 2021).

Any illegal conduct using a system, piece of technology, or network is known as cybercrime. Cybercrimes may be broadly classified into two categories: those that intentionally attack systems and those that unintentionally contribute to systemic crimes. Cybercriminals frequently employ the techniques indicated in Table 3. The three pillars of confidentiality, integrity, and availability form the foundation of every organization's security. Since the first computer systems (see Fig. 6), these three concepts have been known as the security triangle, or CIA, and have been the industry standard for systems security. (Palmieri et al., 2021). Exclusive access to sensitive information and functions is mandated under the concept of secrecy. For instance: Confidentiality of military secrets.

According to integrity principles, only resources and people with permission are able to add, edit, or remove sensitive data and features. Example: Incorrect data is entered into a database by Auser (Integrity). According to Availability Principles, data, systems, and functions must be available when needed within predetermined boundaries based on Service Level Agreements (Availability) (Nguyen and Golman, 2021).

The most effective cyber-security techniques defy the previously established criteria. A skilled hacker may easily get past this simple defense. A company's growth increases the difficulty of cyber-security. Treating the increasing number of participants in the real and virtual worlds of data interchange is another cyber-security constraint. One significant obstacle in the field of cyber-security is the lack of qualified personnel. Many persons with broad capabilities are at the bottom end of the cyber-security spectrum. Coverage of cyberspace is extensive.

We will review the primary categories of cyber security in the article that follows.

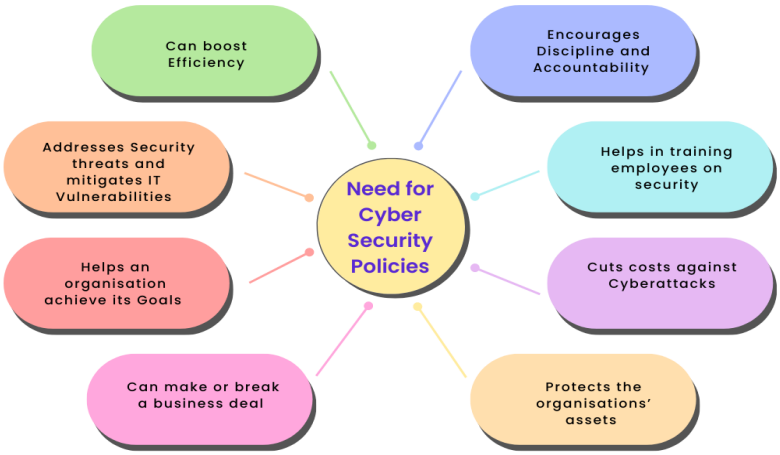
Comprehensive strategies address each of these factors and don't leave any out (Alzubaidi, 2021).The primary physical and cyber infrastructure in the world functions together. This amazing construction offers us several advantages. Nevertheless, putting an online system into place exposes it to additional hacking and cyber attack risks. Decision-makers inside the organization must take into account how assaults could impact their performance. A number of the most skilled cybercriminals believe that web application security is the weakest link in an organization's defense. First, strong encryption is essential for application security.

Every strategy needs to be specifically created and implemented for every type of business. This makes information hacking and infiltration less common. The complexity of cyber-security is rising. Organizations must understand cyber-security from a "security perspective." To stay one step ahead of hackers, you must thus constantly have good security. The increase in security risks has led to a rise in investments in cyber-security systems and services. McAfee, Cisco, and Trend Micro are the three businesses that are involved in this industry (Chandra and Snowe, 2020).

Cyber-security policy- Over time, cyber has efficiently dispersed knowledge and raised communal produce. No matter what sector or application cyber is employed in, there has always been a thought to increase output. System security is largely compromised by rapid data flow to the internet. Security gauges are rapidly in ‘direct opposition’ to development for IT professionals who increase productivity since preventive indicators limit, forbid, or postpone user access, consume indicators that identify vital system resources, and need managerial attention (Katrakazaset al., 2020). The system is updated with timely and appropriate system hardware. The tension that exists along the cyber-security strategy between the need for cyber performance and the security situation is crucial.

The term "policy" relates to a number of topics connected to cyber-security, including system operations plans for technological control, private sector objectives for data conservation, and information dissemination laws and regulations. Nonetheless, there are several uses of the phrase "cyber-security policy" in this sector of work. Similar to "cyberspace," "cyber-security policy" lacks a set meaning; nonetheless, when this term is employed as an adjective in the context of policy, a shared understanding is meant (Tam et al., 2021).

www.ijprems.com
editor@ijprems.com
INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 04, Issue 10, October 2024, pp : 673-679
e-ISSN : 2583-1062
Impact Factor : 7.001



Only the relevant areas of the regulator are formally covered by the cyber-security policy, which has been approved by the regulatory framework. Policy spectrum influences the components of security policies, which differ (Cheng et al., 2020). For instance, the "national cyber-security" policy covers "all citizens and maybe international" businesspeople operating in the same industry; however, corporate cyber-security is limited to personnel who are legally hired or have a contract in place, and who are required to behave responsibly towards the organization. In the absence of a written contract, resource suppliers who depend only on a single client cannot be expected to comply with the 'customer security policy'. The method by which objectives made policies and the mechanism by which policies are enshrined in laws differ in governance. However, centralized security units in businesses are frequently in charge of cyber-security policies, standards, and associated solutions. The security unit's "standards and solutions" serve as the rules' compass in businesses. The "cyber-security policy" released by the many internal units of the common components wing is alternate indication of an organization that places a high importance on security. These shared elements can occasionally be used to spot policy inconsistencies that arise from attempting to address several problems at once (Quigley et al., 2015).

Cyber security policy in the nation is now a subset of national security policy. Laws and regulations of this kind are not as sovereign as the constitution, even if we take into account a "nation's cyber-security strategy" in accordance with the economic or "State Department" policies. In actuality, debates and discussions on many topics lead to the creation and publication of policies in papers and lectures. To direct and make decisions on laws and regulations, policies are developed. Regulations and rules have no bearing on the policy itself. Rules, agreements, and laws, at their finest, constitute a sensible and significant policy. Nonetheless, without developing a cyber-security strategy, directives, guidelines, and regulations can be offered for 'cyber-security enforcement' "Sakhnini et al., 2021".

Within the corporate setting, various divisions are expected to adhere to the regulations out of concern for penalties, which will linger until the offending industry shuts down. Human resource, civil, and costing policies, for example, is designed such that any violation of the notification guidelines results in the closure of the relevant part. Middle managers are supposed to produce indicators at the departmental level to evaluate policy compliance and to integrate communication policies into departmental actions, such as employing people and submitting costs. Any kind of organizational division in the public sector must contend with governance restrictions (Baig et al., 2017). There are certain exceptions, where some information classification sections are handled extremely seriously; nonetheless, the business security policy that the CEO provides applies to the whole firm, while the security policy that the CEO issues is restricted to the domain. Technology staff is applicable. A recent shift in the organizational landscape is the appointment of a senior manager or senior data security manager to oversee the selection of various aspects of an organization's security posture.

Furthermore, the fact that corporate cyber-security policy is entrusted to middle management is another unfavorable distinction from human resource or legal policy. When there is a significant danger of private information being disclosed, information should not be given without carefully assessing the recipient's capacity to preserve information security, according to cyber-security policy (Arendetal., 2020).This policy leaves the management of data risk assessment to them. The manager may choose to cut expenses by outsourcing the flow of information into the office and hiring outside contractors to do information analysis. It's possible that the manager intends to cut expenses by avoiding examination. Such a scenario arises from either an incorrect assessment of information duties to a non-security specialist or maybe from the risk-bearing culture of the organization in issue. In all cases, work division is crucial. The complexity and difficulty of these circumstances increase because indicators related to human resources or accounting have advanced more than cyber-security measures.

2. CONCLUSION

One of the most significant power sources of the third millennium is the internet and related technologies. Because of the characteristics of cyberspace—low entry costs, anonymity, vulnerability, and asymmetry—power dissipation has become a phenomenon. This means that if governments have so far divided the power struggle among themselves, then other actors—private enterprises, criminal organizations, organized terror groups and individuals—must be involved, even though governments continue to play a significant role in this. Obviously, the government will not be deprived of their national security by these phenomena. There are several methods to assess this impact. The idea of security comes first. The danger to national security nowadays is not limited to military matters or boundaries, but also includes the possibility of people' quality of life deteriorating. The second is that cyber dangers no longer have a geographic component. Formerly, military dangers were limited to a certain area. That made it easy to deal with, at least in terms of identification. The third is the degree to which cyber threats have exposed vulnerabilities. These dangers are multifaceted, irregular, and have a very high potential for harm as they are connected to delicate networks and infrastructure. Fourth, governments alone are insufficient to confront these dangers; government and private sector collaboration, which has mutual interests in addressing them, is necessary for effective and bilateral containment. These threats cannot be controlled by traditional tactics alone, such as the deployment of military and police power. He demands to be met with such threats. Fifth, individuals and businesses are not immune to the negative effects of cyber threats, as the preceding point illustrates. Cyber risks are not just available to governments. Sixth, the many international relations theories whose foundations are mostly centered on government are easily disregarded or misunderstood as security in the digital age is not exclusive to governments.

3. REFERENCES

[1] Chen,J.-K., et al., 2021. Cyber deviance among adolescents in Taiwan: Prevalence and correlates. Child. Youth Serv.Rev.126,106042.

[2] Cheng,S., et al., 2020. A new hybrid solar photovoltaic / phosphoric acid fuel cell and energy storage system; Energy and exergy performance. Int. J.Hydrogen Energy.

[3] Damon, E.,et al., 2014. Cyber security education: The merits of firewall exercises. In: Akhgar, B., Arabnia, H.R. (Eds.), Emerging Trends in ICT Security. Morgan Kaufmann, Boston,pp.507–516(Chapter31).

[4] Dash,N., Chakravarty, S., Satpathy, S., 2021. An improved harmony search based extreme learning machine for intrusion detection system. Mater. Today:Proc..

[5] Edgar,T.W.,Manz,D.O.,2017.Science and cyber security. In:Edgar,T.W., Manz,D.O.(Eds.), Research Methods for Cyber Security.Syngress,pp.33–62(Chapter2).

[6] Furnell,S., Shah, J.N., 2020. Home working and cyber security – an outbreak of un preparedness? Comput. Fraud Secur.2020(8),6–12.

[7] Furnell,S.,etal.,2020.Understanding the full cost of cyber security breaches. Comput. Fraud Secur.2020 (12),6–12.

[8] Gupta Bhol,S., Mohanty, J.R.,Kumar Pattnaik,P., 2021. Taxonomy of cyber security metricsto measure strength of cyber security. Mater.Today:Proc..

[9] Hart,S., et al., 2020. Riskio: A serious game for cyber security awareness and education.Comput.Secur.95,101827.

[10] Huang,J.,etal.,2020.Securere motestate estimation against linear man-in-the middle attacks using water marking. Automatica121,109182.

[11] Iqbal,Z., Anwar, Z., 2020. SCERM—A novel framework for automated management of cyber threat response activities. Future Gener. Comput. Syst. 108,687–708.

[12] ji,Z.,etal.,2021. Harmonizing safety and security risk analysis and prevention in cyber–physical systems. Process Saf.Environ.Prot.148,1279–1291.

[13] Snehi,M., Bhandari, A., 2021. Vulnerability retrospection of security solutions for software-defined cyber–Physical system against DDoS and IoT-DDoS attacks.Comp.Sci.Rev.40,100371.

[14] Solomon,R.,2017. Electronic protests: Hacktivismasa for mofpro test in Uganda. Comput. LawSecur.Rev.33(5),718–728.

[15] Sun,C.-C.,Hahn,A.,Liu,C.-C.,2018.Cybersecurityofapowergrid:State-of-the art. Int. J.Electr. Power Energy Syst.99,45–56.

[16] Tam, T.,Rao, A.,Hall, J.,2021. The bad and the missing: An arrativere view of cyber-security implications for Australian small businesses. Comput. Secur.102385.

[17] Tan,S., et al., 2021. Attack detection design for dc microgrid using eigen value assignment approach. Energy Rep.7,469–476.

[18] Thomson, J. R.,2015. Cyber security, cyber-attack and cyber-espionage. In: Thom-son, J.R. (Ed.), High Integrity Systems and Safety Management in Hazardous Industries. Butterworth-Heinemann, Boston,pp.45–

53(Chapter3).

[19] Topping, C.,etal.,2021. Beware suppliers bearing gifts!: Analyzing coverage of supply chain cyber security in critical national in frastructures ectorial and cross sectorial frameworks. Comput.Secur.108,102324.

[20] Tosun,O.K.,2021.Cyber-attacks and stockmarketactivity.Int.Rev.Financ.Anal.76,101795. Varga,S.,Brynielsson,J.,Franke,U.,2021.Cyber-threat perception and risk management in the Swedish financial sector.Comput.Secur.105,102239.

[21] Amir,M., Givargis, T., 2020. Pareto optimal design space exploration of cyber–physical systems. Internet Things 12, 100308.

[22] Arend,I., et al., 2020. Passive- and not active-risk tendencies predictcybersecuritybehavior.Comput.Secur.97,101964.

[23] Ashraf,J., et al., 2021. IoTBoT-IDS: A novel statistical learning-enabled botnet detection framework for protecting networks of smart cities.SustainableCitiesSoc.72,103041.

[24] Aziz,A.A., Amtul, Z., 2019. Developing Trojan horses to induce, diagnose and suppress Alzheimer'spathology.Pharmacol.Res.149,104471.

[25] Baig,Z.A., et al., 2017. Future challenges for smart cities: Cyber-security and digital forensics. Digit.Investig.22,3–13.

[26] Beechey,M., Kyriakopoulos, K.G., Lambotharan, S., 2021. Evidential classification and feature selection for cyber-threat hunting. Knowl.-Based Syst. 226,107120.

[27] Bullock,J.A., Haddow, G.D., Coppola, D.P., 2021. Cyber security and critical infrastructure protection. In: Bullock, J.A., Haddow, G.D., Coppola, D.P.(Eds.),Introduction to Homeland Security, sixth ed. Butterworth-Heinemann, pp.425–497(Chapter8).

[28] Cao,Y., et al., 2019. A topology-aware access control model for collaborative cyber–physical spaces: Specification and verification. Comput. Secur. 87,101478.

[29] Cao,J., et al., 2021. Hybrid-triggered-based security controller design for net-worked control system under multiple cyberattacks.Inform.Sci.548,69–84.