IJRRS
International Journal of Reliability, Risk and Safety: Theory and Application

Online ISSN: 2676-3346

OPEN ACCESS

Vol. 6/ Issue 2/ 2023/ pp. 77-83
DOI: 10.22034/IJRRS.2023.6.2.9
Received: 02 October 2023, Revised: 06 December 2023, Accepted: 06 December 2023
Available online at: https://www.ijrrs.com

Review Article

Origins of Cyber Security: Short Report

Ashkan Kazemi[1*], Mohsen Kalhornia Golkar[2] and Shakib Lajmiri[3]

1- Iranian Social Security Organization, Shiraz, Iran
2- Department of Psychology, Human Science Faculty, Islamic Azad University, Ghods City Branch, Iran
3- Department of Educational Management, Human Science Faculty, Islamic Azad University, Ahvaz Branch, Iran
*** kazemi_psy@yahoo.com**

Abstract

Security is the most basic need of any society and the most important factor for the sustainability of social life; therefore, it has been the focus of experts and theorists since the distant past. The spread of the Internet, new information and communication technologies, and the communication revolution have created a new type of virtual communication devoid of the spirit that governs real social relations. This has caused the emergence and formation of cyberspace parallel to the real world and has disrupted the equations and patterns of traditional communication, production, transfer, and consumption of information and has caused a global movement in the field of communication and transfer of content and communication messages in the fastest possible time. Therefore, as human life is mixed with the cyber revolution, cyber security has come. Cyber security is security in the infrastructure and information arteries, and creating new opportunities for jobs and countries in the environment of automation, electronic commerce, exchange, and cooperation has led to targeted production, storage, and exploitation of sensitive and vital information. In general, different aspects of citizens' lives are mixed with cyberspace, and any instability, insecurity and challenges in this space directly affect different aspects of citizens' lives, especially their security.

Keywords: Cyber; Security; Origin; Virtual Space.

1. Introduction

"Security" is the most basic need of every society and the most important factor for the durability of social life. Therefore, it has been the focus of experts and theorists since the distant past [1]. The concept of security has been changed under the influence of international macro-level developments, and with the start of the globalization process and under the influence of information and communication technology, it has gained a multidimensional concept [2]. On the other hand, it has become a fundamental concept and is one of the necessities of human life. Throughout history, humans have searched for safe and risk-free conditions and tried different ways to achieve them. It can be said that the first social institutions were also formed in response to this need; Hence, security is recognized as one of the main building blocks of social life. In addition to the fact that people and ordinary people have recognized the importance of security in their personal and public lives, most researchers in various scientific fields also point to its importance and believe that security is one of every person's essential and basic needs [3]. The sustainability of societies depends on security, and in its absence, chaos will be the scene's reality. Many theoreticians, from Khwaja Nizam al-Molk to Beyhaqi and Ghazali, Hobbes, Badan, and Machiavelli, have defended security and its necessity in societies, even defending autocrats. They are afraid of disorder and insecurity, which distorts the social foundations, and in response to this human need and proof of social order, they have presented their theoretical discourses. Security also has a special place in Islamic thought. For example, it is stated in the Prophet's hadith that: "Security and health are two blessings that many people are lacking." Some believe that there is a time when there is no threat in society. Therefore, insecurity

How to cite this article:
A. Kazemi, M. Kalhornia Golkar and Sh. Lajmiri, "Origins of Cyber Security: Short Report," *International Journal of Reliability, Risk and Safety: Theory and Application*, vol. 6, no. 2, pp. 77-83, 2023.

is the basis of research and how to control it by increasing military power. Some others have defined security as synonymous with the state of peace and believe that security has a security aspect and that the absence of threats to a country's national interests is equal to security. In addition, some thinkers, such as "Galtang", have proposed the concept of "reassuring security" and considered security synonymous with eradicating violence from human societies. Therefore, every political system considers its most important duty to create and maintain security and deal with any threat that endangers its security. Eliminating risks by any government is reasonable, mandatory, and worthy [1].

On the other hand, today, the spread of the Internet, new information and communication technologies, and the revolution of communication have created a new type of virtual communication devoid of the spirit governing real social relations. This caused the emergence and formation of cyberspace parallel to the real world and disrupted the equations and patterns of traditional communication, production, transmission, and consumption of information and caused a global movement in the field of communication and transmission of content and communication messages in the fastest possible time [4, 5].

Such a space, considered an integrated cyber reality, has eliminated some of the most important and cumbersome limitations in the physical world and has created an attractive environment for its users, leading to the deception of users and distortions in their attitudes [4]. Through the magnification of the capabilities or, in other words, drowning in the attractions of cyber realities, it is the ground for the occurrence of cyber anomalies and many crimes in complex and new forms. As a result, we witness the emergence of a kind of conflict between the behavior of users in cyberspace and the real world. So, in the blink of an eye, horrible crimes occur in cyberspace, which sometimes leads to the death of the victims [6, 7].

Cyberspace has had such a fundamental impact on societies that human life is unimaginable without it. In fact, the influence of the cyber revolution on human life is so wide that some even evaluate it beyond the invention of the line and the beginning of human civilization. However, it is indisputable that the cyber revolution has created a wave that changes a new aspect of human life every day and gives it a new shape [8]. As human life merges with the cyber revolution, cyber security comes up. Cyber security is security in infrastructure and information arteries. Creating new opportunities for jobs and countries in the automation, e-commerce, exchange, and collaboration environment has led to targeted production, storage, and exploitation of sensitive and vital information. Dependence on high-speed networks and the power of processors is increasing daily, which exposes systems to natural risks and even crime and cyber terrorism, which requires monitoring and management [9].

In most recent studies, Cybersecurity is defined as a comprehensive term [10]. ITU-T X.1205 also defines cybersecurity in its draft [11]. Hence, in generalized terms, cyber security helps prevent cyberattacks and data breaches and can aid in risk management. Security architecture defines some security characteristics, including security attacks of two types: active and passive attacks and security objectives [12].

In general, the threats include various scenarios such as Cyberbullying [13], Identity theft [14], Digital devices [13], Autonomous systems [15], (Wireless Sensor Networks (WSN), and Wireless body area Networks (WBAN) [16], Cyber terrorism [13], and can approach us from unforeseen sources and directions. With the advancements in science, more sophisticated cyber-crimes and malicious activities are evident in today’s world, which is targeted and extremely dangerous. One such example was detected earlier in 2018; a ransomware attack was harming the government of Atlanta City [17], as well as other recent cyber breaches [18].

On the other hand, we live in the era of the Internet revolution. Shortly, the whole global population will be accessing the Internet. The Internet of Things (IoT) is the gateway to communicating with humans to machines (H2M) and machine-to-machine (M2M). In IoT, different devices are connected via IP-based solutions through the Internet. Cisco reported that 29.3 billion devices will be connected to the Internet by 2023 (The Cisco Annual Internet Report, 1490). Home appliances like televisions, fridges, mobiles, laptops, personal computers, and even motorcycles and cars have small-scale non-IP-based solutions. The IoT aims to connect all kinds of devices at a small or large-scale business standard that can directly communicate with IP addresses through the Internet [19].

IoT is making it easy to access pollution monitoring; smart houses, smart buildings, smart cities, intelligent transportation, healthcare centers, and smart grids (SG) are the most significant application sectors [20]. The SG consists of a power and communication line between the generation and demand sides. Therefore, intercommunication is very important for SG to communicate with energy generation and demand-side management [21]. In an SG system (SGS), bidirectional communication devices such as sensors

and meters are used to measure energy generation and consumption on the demand side [21]. This simplifies delivering a real-time monitor, control, and balance everywhere at a higher accuracy [22].

Adopting information and communication technology (ICT) for cyber-physical system upgrading has created a conducive environment for cyber components. Cyberattacks threaten cyber-physical system sustainability and security concerns [23]. According to recent research, a cyberattack on the cyber-physical system disrupted the grid control and functioning system. Nodal price manipulation or False Data Injection (FDI) might mislead state estimation. This devastated the SG cyber-physical system market. A Denial of Service (DoS) cyber-attack may affect the SG cyber-physical system's dynamic performance [23, 24]. Before deploying in the existing cyber-physical system, it is important to evaluate device applications, algorithms, and settings [19].

Recently, ChatGPT has achieved a momentous change and made substantial progress in natural language processing. As such, a chatbot-driven AI technology can interact and communicate with users and generate human-like responses. ChatGPT, on the other hand, can potentially influence changes in the cybersecurity domain. ChatGPT can be utilized as a chatbot-driven security assistant for penetration testing to analyze, investigate, and develop security solutions. However, ChatGPT raises concerns about how the tool can be used for cybercrime and malicious activities. Attackers can use such a tool to cause substantial harm by exploiting vulnerabilities, writing malicious code, and circumventing security measures on a targeted system [25].

The world is experiencing rapid growth in cyberspace today [26]. Such an extraordinary growth in information- access gives opportunities to those with malicious intentions. It is the need of the hour [26] and the act of protecting the systems and technologies from unusual activities. Cyber security means maintaining the Integrity, Confidentiality, and Availability (ICA) of computing assets belonging to an organization or connecting to another organization’s network. Due to the evolution and increase of cyber threats, many researchers believed and urged to educate the new generation about cyber-security concepts [27]. Cyber crimes occur due to negligence in cyber-security and client awareness [19]. Recent research [28, 29] states that the US has introduced threat intelligence frameworks. This framework works on gathering information from various sources that human security experts have carefully examined. Besides, the researcher also uses machine learning techniques to analyze threats that, in an advanced way, respond to attack incidents [30]. The United Kingdom has introduced its own National Cyber Security Strategy 2016–2021 that resembles the ideas of the 2011 version [31] and has allocated a budget of £1.9bn for the Cyber Security Programme [32]. At least 70 nations have addressed this issue through national cyber/information security strategies and significant legal acts in some strategy documents describing their national security and defense strategies [33]. In fact, under the cyber network guide, the preplanning of vulnerabilities includes the timely information exchange regarding threats, which may lead to the protection of various entities such as the environment, business, and infrastructure and is capable of understanding the situational incidents accordingly [34].

We live in the digital age, which, like anything else, has its upsides and downsides. The main drawback is the security risk [35, 36]. Security breaches are becoming more common and catastrophic as more sensitive information transfers to the digital arena. Cyber-criminals are growing more adept in their attempts to avoid detection, and many newer malware kits are already incorporating new ways to get out of antivirus and other threat detection systems. Cybersecurity, on the other hand, is at a crossroads, and future research efforts should be focused on cyber-attack prediction systems that can foresee important scenarios and consequences rather than depending on defensive solutions and focusing on mitigation. Systems that are based on a complete, predictive study of cyber risks are required all around the world. The key functionalities in cybersecurity, such as prediction, prevention, identification or detection, and corresponding incident response, should be done intelligently and automatically. Artificial intelligence (AI), which is based primarily on Machine Learning (ML) [37, 38], is capable of recognizing patterns and predicting future moves based on prior experiences, thereby preventing or detecting potentially malicious activity.

In Figure 1, the process flowchart of cyber security risk assessment design by "BB ABILITY™ CYBER SECURIT Y SERVICES" was shown

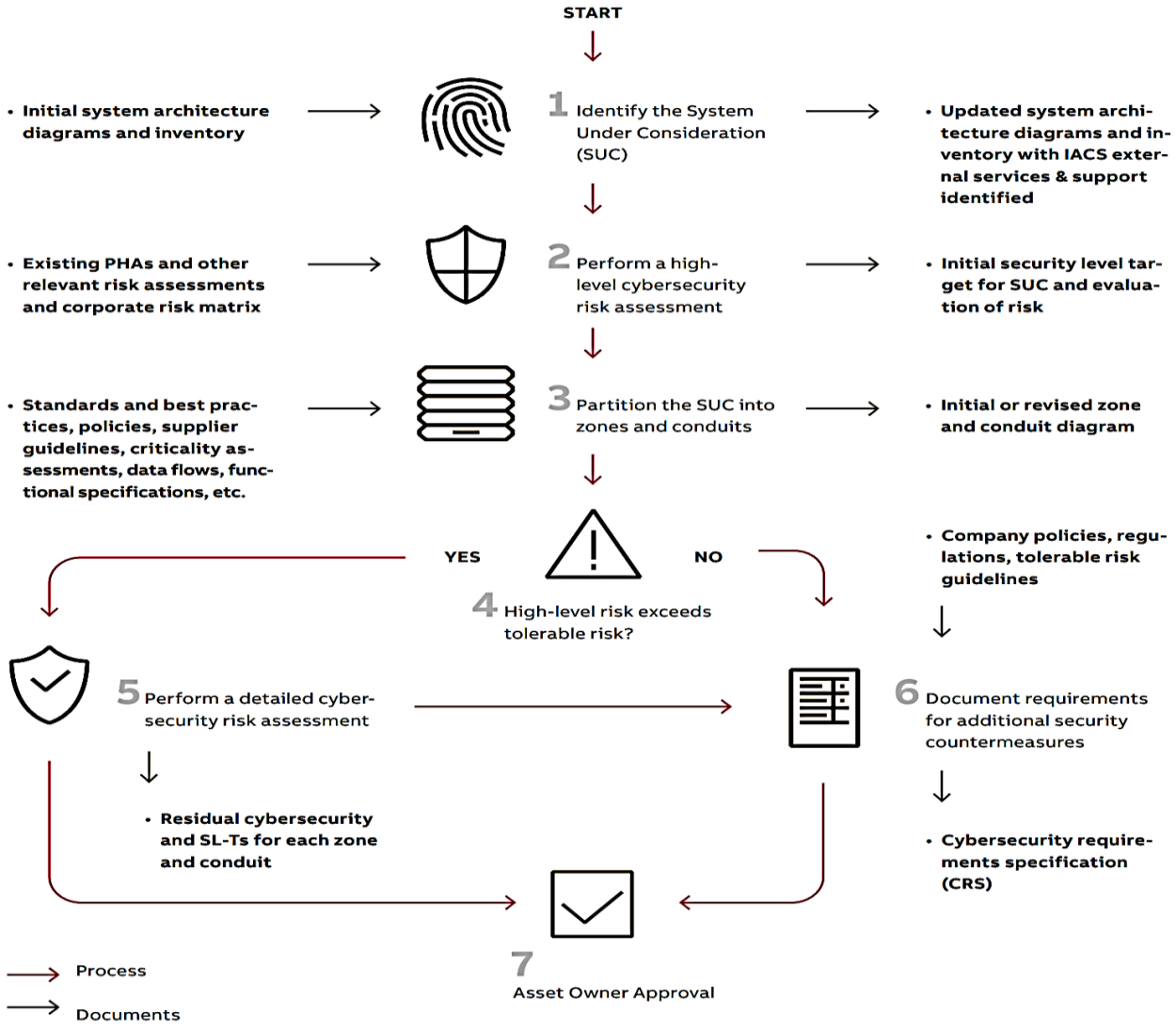

Figure 1. the process flowchart of cyber security risks assessment

An existing research gap is related to the origin of the emerging cybersecurity concept. Because the researchers of this article did not find comprehensive and complete texts related to the origin of this concept in reliable scientific sites and Iranian and non-Iranian books. Therefore, considering that the present study is in the security field, it seeks to answer the question, where did the emerging concept of cyber security come from?

2. Method

The current study is in the framework of a short report. It aims to discover the origin of the cyber security concept by reviewing the contents of the cyber and security field. Therefore, the collection of articles published inside and outside the country related to the last 2 years in the cyber security field was examined. The keywords used for the search were "security and cyber" (There are reliable databases such as sid.ir, ensani.ir, magiran.com, civilica.ir, scholar.google.com, and sciencedirect.com).

3. Finding

The findings from all the reviewed articles have indicated that in domestic research, other forms of security such as perceptual security [39], social security [40,41], cultural security [3], environmental security [42], national security [43], economic security [44], Human security [45] and cyber security [46-49] have been observed. Social security and cyber security have been the subject of much research.

According to the findings, the Types of cybersecurity threats are as follows:

3.1 Phishing

Phishing is the practice of sending fraudulent emails that resemble emails from reputable sources. The aim is to

steal sensitive data like credit card numbers and login information. It is the most common type of cyber attack. You can help protect yourself through education or a technology solution that filters malicious emails.

3.2 Social engineering

Social engineering is a tactic that adversaries use to trick you into revealing sensitive information. They can solicit a monetary payment or gain access to your confidential data. Social engineering can be combined with any of the threats listed above to make you more likely to click on links, download malware, or trust a malicious source.

3.3 Ransomware

Ransomware is a type of malicious software. It is designed to extort money by blocking access to files or the computer system until the ransom is paid. Paying the ransom does not guarantee that the files will be recovered or the system restored.

3.4 Malware

Malware is a type of software designed to gain unauthorizedaccess or to cause damage to a computer.

4. Conclusion

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks usually aim to access, change, or destroy sensitive information, extort money from users via ransomware, or interrupt normal business processes. Implementing effective cybersecurity measures is particularly challenging today because there are more devices than people, and attackers are becoming more innovative.

A successful cybersecurity approach has multiple layers of protection spread across the computers, networks, programs, or data one intends to keep safe. In an organization, the people, processes, and technology must complement one another to create an effective cyberattack defense. A unified threat management system can automate integrations across select Cisco Security products and accelerate key security operations functions: detection, investigation, and remediation.

Users must understand and comply with basic data security principles like choosing strong passwords, being wary of attachments in email, and backing up data.

Organizations must have a framework for dealing with attempted and successful cyberattacks. One well-respected framework can guide you. It explains how you can identify attacks, protect systems, detect and respond to threats, and recover from successful attacks. Technology is essential to giving organizations and individuals the computer security tools to protect themselves from cyberattacks. Three main entities must be protected: endpoint devices like computers, smart devices, routers, networks, and the cloud. Common technologies that protect these entities include next-generation firewalls, DNS filtering, malware protection, antivirus software, and email security solutions.

In today's connected world, everyone benefits from advanced cyberdefense programs. At an individual level, a cybersecurity attack can result in everything from identity theft to extortion attempts to the loss of important data like family photos. Everyone relies on critical infrastructure like power plants, hospitals, and financial service companies. Securing these and other organizations is essential to keeping our society functioning.

Everyone also benefits from the work of cyber threat researchers, like the team of 250 threat researchers at Talos, who investigate new and emerging threats and cyber attack strategies. They reveal new vulnerabilities, educate the public on the importance of cybersecurity, and strengthen open-source tools. Their work makes the Internet safer for everyone.

The ever-increasing development of the global Internet network and the expansion of the digital economy and virtual society make the existence of a new society with new social and psychological coordinates certain. One of the basic requirements of this "information society" and "network society" and the new attractive world is the feeling of security and peace of mind of users and communities. Entering the age of information, digital and virtual spaces, and the opportunities and risks arising from it have reduced the importance of feeling safe and doubled its necessity.

5. References

[1] A. Gurbanpour and M. Gurbanpour, "The concept of national security and the role of the constitution of the Islamic Republic of Iran in providing it," *the first festival of the best scientific works of Islamic humanities*, Allameh Jafari special award, 2018, [online]. Available: https://www.sid.ir/paper/899421/fa (in Persian).

[2] A. Abedi,"Investigating the concept of cyber security," *the second national cyber defense conference*, Maragheh, 2019, [online]. Available: https://civilica.com/doc/903740/ (in Persian).

[3] S. Sharifi Rahnmo, A. Fathi, E. Emrani, M. Sharif irahnmo, B. Zare kohan and M. Ebrahimi, "Forecasting Components of Youth Cultural Security based on the Degree of Attachment to Cyberspace," *Societal Security Studies*, vol. 12, no. 65, pp. 69-88, 2021, [Online]. Available: https://www.magiran.com/paper/2283781 (in Persian).

[4] L. De Kimpe, K. Ponnet, M. Walrave, T. Snaphaan, L. Pauwels and W. Hardyns, "Help, I need somebody: Examining the antecedents of social support seeking among cybercrime victims," *Computers in human behavior*, vol. 108, pp. 106310, 2020, doi: https://doi.org/10.1016/j.chb.2020.106310

[5] M.C.B. Umanailo, I. Fachruddin, D. Mayasari, R. Kurniawan, D.N. Agustin, R. Ganefwati and R. Fitriana, "Cybercrime case as impact development of communication technology that troubling society," *Int. J. Sci. Technol. Res*, vol. 8, no. 9, pp. 1224-1228, 2019,

[Online]. Available: http://repository.unisbablitar.ac.id/id/eprint/703

[6] H. Sayyadi Tooranloo, H. Mirghafoori, M. Mahdavi and S. Saghafi, "Analysis of factors related to the establishment of Cybercrime using a Fuzzy approach," *Order & Security Research Journal*, vol. 13, no. 3, pp. 27-54, 2020, [Online]. Available: https://www.magiran.com/paper/2169236/ [in (in Persian).

[7] Z. Jahbin, A. Mozaffari, N. Hashemzehi and S.M. Daddaran, "Qualitative study of the causes of criminality in cyberspace (qualitative analysis of cybercrime cases)," *Journal of Socio - Cultural Changes*, vol. 15, no. 4, pp. 48-71, 2019, [Online]. Available: https://journal.khalkhal.iau.ir/article_664263.html (in Persian).

[8] G. Toraby and M.N. Taherizadeh, "The Cyber Revolution and The Evolution of the Concept of Information Warfare in the Field of International Relations," *International Studies Journal (ISJ)*, vol. 17, no. 4, pp. 47-65, 2021, doi: 10.22034/isj.2021.279939.1432 (in Persian).

[9] E. Katanchi and B. Pourghahramani, "Cyber Security Challenges in ASEAN Countries," *International Studies Journal (ISJ*), vol. 18, no. 1, pp.139-156, 2021, doi: 10.22034/isj.2021.252695.1237 (in Persian).

[10] ISO, "*Guidelines for Cyber Security*," 2018, [Online]. Available: http://www.iso27001security.com/html/27032.html.

[11] International Telecommunications Union (ITU). X. 1205: "*Overview of Cyber Security*," 2018, [Online]. Available: https://www.itu.int/rec/T-REC-X.1205-200804-I

[12] W. Stallings, "Cryptography and network security, 4/E," *Pearson Education India*, 2006, [Online]. Available: http://hdl.handle.net/1/5304

[13] DM. Smit, "Cyberbullying in South African and American schools: A legal comparative study," *South African Journal of Education*, Vol. 1, no. 35(2), pp. 1-1, 2015, doi: 10.15700/saje.v35n2a1076

[14] E. Michel, ME. Kabay, E. Salveggio, R. Guess and RD. Rosco, "*Computer Security Handbook (6th ed.)*," Wiley [Online Library], 2015, ISBN: 9781118134115.

[15] S. Parkinson, P. Ward, K. Wilson and J. Miller, "Cyber threats facing autonomous and connected vehicles: Future challenges," *IEEE transactions on intelligent transportation systems*, Vol. 6, no. 18(11), pp. 2898-915, 2017, doi: 10.1109/TITS.2017.2665968

[16] M. Roy, C. Chowdhury and N. Aslam, "Security and privacy issues in wireless sensor and body area networks. Handbook of Computer Networks and Cyber Security," *Principles and Paradigms*, Vol. 1, no. 1, pp. 173-200, 2020, [Online]. Available: doi: 10.1007/978-3-030-22277-2_7

[17] M. Conti, T. Dargahi and A. Dehghantanha, "Cyber threat intelligence: challenges and opportunities," *Springer International Publishing*, 2018, doi:10.1007/978-3-319-73951-9_1

[18] J. Ruohonen, "An acid test for Europeanization: Public cyber security procurement in the European Union," *European Journal for Security Research*, Vol. 5, no. 2, pp. 349-77, 2020, doi: 10.1007/s41125-019-00053-w

[19] MK. Hasan, AA. Habib, Z. Shukur, F. Ibrahim and S. Islam, "Razzaque. Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations," *Journal of Network and Computer Applications*, Vol. 1, no. 209, pp. 103540, 2023, doi: https://doi.org/10.1016/j.jnca.2022.103540

[20] DB. Avancini, JJ. Rodrigues, RA. Rabêlo, AK. Das, S. Kozlov and P. Solic, "A new IoT-based smart energy meter for smart grids," *International Journal of Energy Research*, Vol. 45, no. 1, pp. 189-202, 2021, doi: https://doi.org/10.1002/er.5177

[21] FE. Abrahamsen and Y. Ai, "Cheffena. Communication technologies for smart grid: A comprehensive survey," Sensors. Vol. 3, no. 21(23), pp. 80-87, 2021, doi: https://doi.org/10.3390/s21238087

[22] S. Ahmed, TM. Gondal, M. Adil, SA. Malik and R. Qureshi, "A survey on communication technologies in smart grid," *In2019 IEEE PES GTD Grand International Conference and Exposition Asia (GTD Asia)*, IEEE. Vol. 1, no. 1, pp. 7-12, 2019, doi: 10.1109/GTDAsia.2019.8715993

[23] RM. Czekster, C. Morisset, AV. Moorsel, JC. Mace, WA. Bassage and JA. Clark, "Cybersecurity Roadmap for active buildings," *InActive Building Energy Systems: Operation and Control. Cham: Springer International Publishing*, Vol. 1, no. 1, pp. 219-249, 2021, doi: 10.1007/978-3-030-79742-3_9

[24] A. Kazemy and M. Hajatipour, "Event-triggered load frequency control of Markovian jump interconnected power systems under denial-of-service attacks," *International Journal of Electrical Power & Energy Systems*, Vol. 1, no. 133, pp. 107250, 2021, doi: https://doi.org/10.1016/j.ijepes.2021.107250

[25] M. Al-Hawawreh, A. Aljuhani and Y. Jararweh, "Chatgpt for cybersecurity: practical applications, challenges, and future directions," *Cluster Computing*, Vol. 26, no. 6, pp. 3421-36, 2023, doi: https://doi.org/10.1007/s10586-023-04124-5

[26] B. Arora, "Exploring and analyzing Internet crimes and their behaviours. Perspectives in Science," Vol. 1, no. 8, pp. 540-2, 2016, doi: https://doi.org/10.1016/j.pisc.2016.06.014

[27] DC. Rowe, BM. Lunt and JJ. Ekstrom, "The role of cyber-security in information technology education," *In Proceedings of the 2011 conference on Information technology education*, Vol. 1, no. 1, pp. 113-122, 2011, doi: https://dl.acm.org/doi/abs/10.1145/2047594.2047628

[28] SE. Jasper, "US cyber threat intelligence sharing frameworks," *International Journal of Intelligence and Counter Intelligence*, vol. 2, no. 30(1), pp. 53-65, 2017, doi: https://doi.org/10.1080/08850607.2016.1230701

[29] TD. Wagner, E. Palomar, K. Mahbub and AE. Abdallah, "A novel trust taxonomy for shared cyber threat intelligence," *Security and Communication Networks*, Vol. 1, no. 1, pp. 1-9, 2018, doi: https://doi.org/10.1155/2018/9634507

[30] TP. Thomas, A. Vijayaraghavan and S. Emmanuel, "Machine Learning and Cybersecurity. In: Machine Learning Approaches in Cyber Security Analytics," *Springer*, Singapore, Vol. 1, no. 1, pp. 37-47, 2020, doi: https://doi.org/10.1007/978-981-15-1706-8_3

[31] R. Von Solms and J. Van Niekerk, "From information security to cyber security," *computers & security*, Vol. 1, no. 38, pp. 97-102, 2013, doi:https://doi.org/10.1016/j.cose.2013.04.004

[32] "UKCyber Security Strategy". *National Cyber Security Strategy 2016 to 2021*, [Online]. Available: https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021.

[33] K. Pipyros, C. Thraskias, L. Mitrou, D. Gritzalis and T. Apostolopoulos, "A new strategy for improving cyber-attacks evaluation in the context of Tallinn Manual," *Computers & Security*, Vol. 1, no. 74, pp. 371-83, 2018, doi: https://doi.org/10.1016/j.cose.2017.04.007

[34] F. Fiedelholtz, "Incident Response and Recovery," *The Cyber Security Network Guide*, Vol. 1, no. 1, pp. 31-8, 2021, doi: https://doi.org/10.1007/978-3-030-61591-8_4.

[35] IH. Sarker, "Smart City Data Science: Towards data-driven smart cities with open research issues," *Internet of Things*, vol. 1, no. 19, pp. 100528, 2022, doi: https://doi.org/10.1016/j.iot.2022.100528

[36] IH. Sarker, AI. Khan, YB. Abushark and F. Alsolami. "Internet of things (iot) security intelligence: a comprehensive overview, machine learning solutions and research directions," *Mobile Networks and Applications*, Vol. 28, no. 1, pp. 296-312, 2023, doi: https://doi.org/10.20944/preprints202203.0087.v1

[37] IH. Sarker, "Machine learning: Algorithms, real-world applications and research directions," *SN computer science*, Vol. 2, no. 3, pp. 160, 2021, doi: 10.1007/s42979-021-00592-x

[38] IH. Sarker, "CyberLearning: Effectiveness analysis of machine learning security modeling to detect cyber-anomalies and multi-attacks," *Internet of Things*, Vol. 1, no. 14, pp. 100393, 2021, doi: https://doi.org/10.1016/j.iot.2021.100393

[39] R. Ghahremani and E. Amini, "Analyzing the Health of Urban Streets with an Emphasis on the Components of Residents' Perceived Safety (Case Study: District 4 of Tehran Municipality)," *Journal of Social Order*, vol. 13, no. 4, pp. 35-62, 2021, doi: 20.1001.1.20086024.1400.13.4.2.2 (in Persian).

[40] M. Niazi, Z. rezvani and Z. Sadeqiarani, "Presenting an interactive model of social security using structural modeling," *Societal Security Studies*, vol. 13, no. 70, pp. 25-49, 2022, doi:10.22034/sss.2022.98069 (in Persian).

[41] MH. Yazdani and M. Jami Odolo, "Assessing the social damage of Covid-19 on the feeling of social security in public spaces (case example: Ardabil city)," *Scientific Quarterly Journal of Social Security Studies*, vol. 13, no. 69, pp. 153-174, 2022, [Online]. Available: https://ecc.isc.ac/showJournal/1957/272215/3453802 (in Persian).

[42] H. Hayaty and L. Nourmohamadi dehbalai, "Assessing and Evaluating Women's Security Factors in Urban Parks Stressing Social Productivity and Surrounding Security (Case Study: Ilam's "Koodak Park")," *Societal Security Studies*, vol. 12, no. 1, pp. 115-140, 2021, [Online]. Available: http://sss.jrl.police.ir/article_96159.html (in Persian).

[43] R. Khalili and H. Mehraban inchebroun, "Identity policy, education and national security in Iran," *Strategic Studies Quarterly*, vol. 24, no. 94, pp. 39-70, 2021, doi: 20.1001.1.17350727.1400.24.94.2.0 (in Persian).

[44] N. Shahbazi, A. Foroutan Ramy and B. Sadeghi Amroubadi, "Transparency and economic security; Functional analysis of intelligence Services," *Strategic Studies Quarterly*, vol. 24, no. 94, pp. 177-217, 2021, doi: 20.1001.1.17350727.1400.24.94.6.4 (in Persian).

[45] A. Seifi, M. Khaleqinejad and H. Rezaiee, "A constructivist approach to the concept of human security," *Strategic Management Studies of National Defence Studies*, vol. 9, no. 34, pp. 161-143, 2019, doi: 20.1001.1.24234621.1398.9.34.5.0 (in Persian).

[46] M. Mohammadi Khanghahi and M.H. Azadi, "Social Cybersecurity (The Role of Social media in Information wars)," *National Security*, vol. 11, no. 41, pp. 131-158, 2021, doi: 20.1001.1.33292538.1400.11.41.5.3 (in Persian).

[47] A.M. Saadatmand, M.R. Karimi Ghohrodi, H. Mohammadi and M. Babak, "Determining the indicators of cyber security evaluation by comparative study method," *National Security*, vol. 11, no. 40, pp. 37-66, 2021, doi:20.1001.1.33292538.1400.11.40.2.8 (in Persian).

[48] H. Kavyani, N. Mirsepassi and G. Memarzadehtehran. "Designing a personnel Competency Model in Cybersecurity," *Strategic Management Studies of National Defence Studies*, vol. 10, no. 41, pp. 298-273, 2021, doi:20.1001.1.24234621.1399.10.41.11.7(in Persian).