Iraqi Journal for Computer Science and Mathematics

Journal Homepage: http://journal.esj.edu.iq/index.php/IJCM
e-ISSN: 2788-7421 p-ISSN: 2958-0544

Towards Artificial Intelligence-Based Cybersecurity: The Practices and ChatGPT Generated Ways to Combat Cybercrime

Maad M. Mijwil[1]*, Mohammad Aljanabi[2,4], ChatGPT[3]

[1]Computer Techniques Engineering Department, Baghdad College of Economic Sciences University, Baghdad, IRAQ
[2]Department of Computer, College of Education, Aliraqia University, Baghdad, IRAQ
[3]Open AI L.L.C., 3180 18th Street, San Francisco, CA 94110, USA
[4]AlSalam university college, Iraq

*Corresponding Author: Maad M. Mijwil

DOI: https://doi.org/10.52866/ijcsm.2023.01.01.0019
Received January2023; Accepted January 2023; Available online January 2023

ABSTRACT: Today, cybersecurity is considered one of the most noteworthy topics that are circulated frequently among companies in order to protect their data from hacking operations. The emergence of cyberspace contributed to the growth of electronic systems. It is a virtual digital space through which interconnection is established between computers and smartphones connected within the Internet of Things environment. This space is critical in building a safe digital environment free of threats and cybercrime. It is only possible to make a digital environment with the presence of cyberspace, which contains modern technologies that make this environment safe and far from unauthorized individuals. Cybersecurity has a wide range of challenges and obstacles in performance, and it is difficult for companies to face them. In this report, the most significant practices, sound, and good strategies will be studied to stop cybercrime and make a digital environment that guarantees data transfers between electronic devices safely and without the presence of malicious software. This report concluded that the procedures provided by cybersecurity are required and must be taken care of and developed.

Keywords: Cybersecurity, Cybercrime, Cyberspace, Artificial Intelligence, Digitalization, ChatGPT.

1. INTRODUCTION

In recent years, cybercrime has become one of the most crucial points circulated between companies, organizations, and individuals, which is considered one of the most serious crimes [1][2]. These crimes pursue to steal data and change the course of computers by manipulating systems and changing protection programs. Cybercrime affects the performance of computers as well as the psychological state of users, as data theft, alteration or deletion is one of the most dangerous procedures that companies face [3][4]. Therefore, these companies seek the use of modern and advanced technologies in developing their systems and protecting their customers' data. Moreover, taking into account all the crucial measures to protect computers and the use of cybersecurity specialists to create cyberspace free of gaps, as well as the use of artificial intelligence techniques in designing the advantages of cyberspace and making it an excellent and sophisticated digital environment [5-7]. Cyberspace is a digital space that creates a way for computers to connect with each other or with other electronic devices within the Internet of Things environment [8-10]. It utilizes artificial intelligence techniques to protect its data against any wrong operations [11-13]. Figure 1 illustrates the cyber threats that institutions may face in the digital environment. Basically, cyberspace consists of three layers, as each layer is linked with the next layer, which is as follows:

- **Physical layer:** It contains companies, networks, computers, servers, and things connected to the Internet. This layer is the area that unauthorised individuals wish to access and control.
- **Logical layer:** It contains applications, programs, and protocols that have been provided or equipped by specialised and trusted parties.
    - **Semi logical layer:** It contains data and information that is not allowed to be viewed or transmitted except by authorized or trusted individuals.

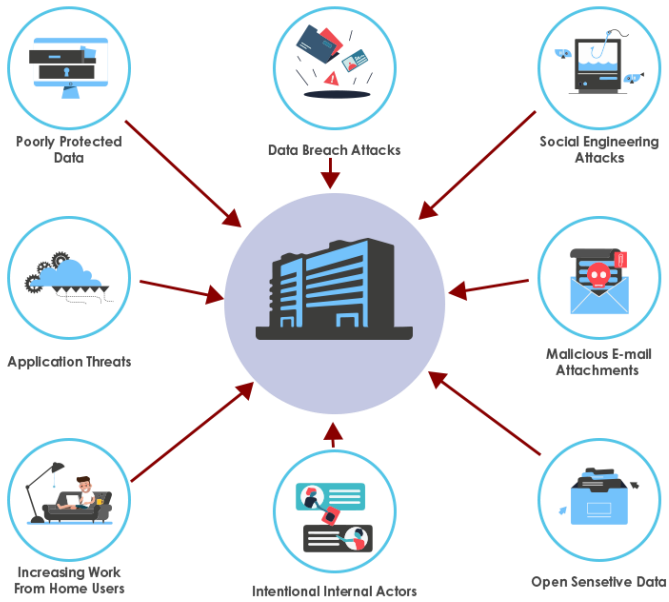

FIGURE 1. - Forms of cyber threats [14].

It must be taken into account that cyberspace has a set of characteristics that must be observed and taken care of so that they are not negative characteristics that affect the work of the digital environment. As the most crucial characteristics are that this space is complex, widespread, and easy to access. This space is where data and information are exchanged through the use of correct and secure practices. In addition, the most crucial feature of this space is that it contains technologies that detect and control complex cyber-attacks and determine the necessary procedures to eliminate these attacks. Cybercrime is a destructive act that significantly affects the functioning of the digital environment through data manipulation, espionage, extortion, or the publication of illegal content targeting clients or companies [15][16]. Electronic crime is considered a serious threat, and quick resolutions must be found for it in the event of its occurrence and control of computer systems. Cybercrime seeks to compromise the security of computers, smartphones, tablets, game consoles, networks, and other things connected to the Internet [17-19]. The perpetrator of a cyber threat can be a person or a group of hackers. Cyber threats have great motives in military espionage, extortion in order to obtain money or information, extortion and ruining people's reputation, revenge and challenge. Therefore, in this article, the most significant measures set by the field of cybersecurity in protecting the digital environment will be reviewed, such as how computers are controlled and not allowed to be damaged or controlled.

2. CYBERSECURITY PRACTICES

Cybersecurity is a set of techniques and approaches that seek to protect computer systems and data from cyber-attacks and not allow malicious software to control the operation of the computer system. It is concerned with securing systems free of loopholes, combating cybercrime, and establishing an excellent electronic environment. Moreover, information must be secured from theft, vandalism, and unauthorized access, as well as protected from natural disasters such as dust, moisture, etc. Companies seek to ensure the integrity of the process of transferring data and information between electronic device systems without the presence of unauthorized third parties working to change, modify or delete data. Confidentiality must exist in a process that seeks to make the process of transferring data and information confidential in order to prevent unauthorized persons from accessing this data through the use of artificial intelligence techniques that facilitate this process without the presence of any obstacles and encrypt it and transfer it to the required party. Computer systems are characterized by their ability to save data or information without changing their content except with the presence of authorized persons, as well as non-repudiation, which is a property to confirm the completion of the required tasks and not to deny a transaction carried out by one of the participants in the digital environment. The execution of computer systems is measured through a set of effective security elements. The six basic elements in the computer information security system must be taken into account, and their influence on data protection measures should be studied (see Figure 2). Moreover, information security systems must be prepared to operate in all cases and under a developed law to combat cybercrime with properly structured and organized management that includes experts in managing information systems.

Cybersecurity concentrates on protecting software and applications from vulnerabilities, which are considered weak points, as they allow cyber-attacks to occur. Cybercriminals focus on weaknesses in information systems by analyzing the practices of these systems and the behavior of users to exploit them in hacking these systems. Phishing is

a type of fraudulent operation through cyberspace that seeks to obtain influential information that benefits cybercriminals through smart mechanisms with the aim of controlling systems and users. Cybersecurity faces many challenges in work practices. Specialists organize information systems in cybersecurity, where standards are set for their use and the conduct of work strategies. The lack of cybersecurity specialists is considered one of the most significant obstacles that companies face, as it is only possible to design a digital environment with a sufficient number of these specialists. The more significant the number of devices connected to the Internet of Things, the more vulnerable cyber-attacks, espionage operations, and the penetration of computer networks. Therefore, companies should have adequate preparations and prepare the necessary technologies to face the threat of cybercrime. Moreover, do not utilize applications or programs from unlicensed or unofficial sites, because these sites may be a reason for hacking operations. Companies must use certain strategies to preserve data and information and make backup copies of them perfectly and accurately. Passwords must be complex and large and must be changed every six months or every year in order to ensure the safety of computer systems. When correct and accurate procedures are used and caution in using websites, the safety of the electronic environment and the satisfaction of companies and customers are guaranteed. The field of cybersecurity contributes to designing a digital environment free of loopholes and not allowing unauthorized persons to enter this environment. These mechanisms can only be achieved with artificial intelligence techniques that play an influential role in changing and controlling cyber-attacks [20-25]. Therefore, the existence of artificial intelligence and effective cybersecurity measures lead to the establishment of a proper digital environment [26-31].

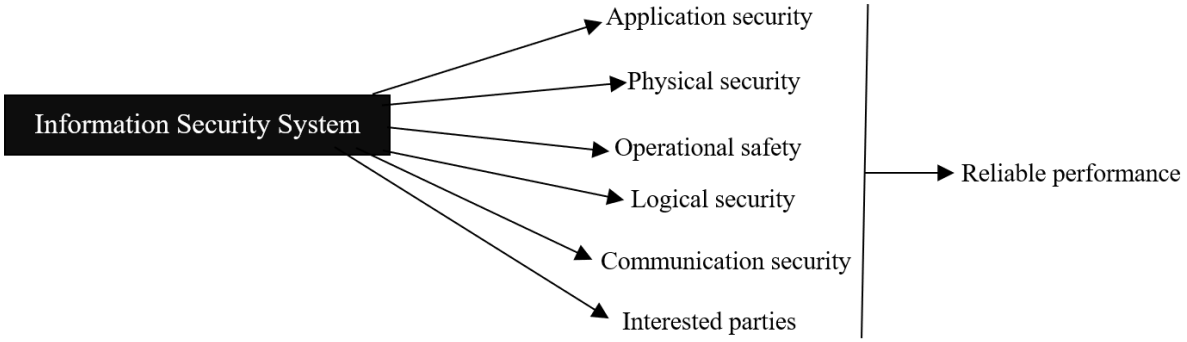

FIGURE 2. – The six main elements for measuring the execution of an information security system.

3. COMBATING CYBERCRIME (by ChatGPT)

Cybersecurity plays a critical role in combating cybercrime by protecting digital systems, networks, and data from unauthorized access, use, disclosure, disruption, modification, or destruction. Cybercrime can take many forms, including hacking, phishing, malware, and ransomware, and can have serious consequences for both individuals and organizations. To combat cybercrime, organizations should implement a comprehensive cybersecurity strategy that includes:

- Regular security assessments: Regularly assess the organization's digital systems and networks to identify vulnerabilities and potential threats.
- Employee education: Provide employees with training on how to identify and prevent cybercrime, as well as how to respond to security incidents.
- Strong authentication: Use strong authentication methods, such as multi-factor authentication, to prevent unauthorized access to digital systems and data.
- Network security: Implement network security measures, such as firewalls and intrusion detection systems, to protect against unauthorized access and attacks.
- Incident response plan: Develop and implement an incident response plan to quickly and effectively respond to security incidents.
- Data encryption: Encrypt sensitive data to protect it from unauthorized access and disclosure.
- Cybersecurity threat intelligence: Continuously monitor the cyber threat landscape and stay informed about the latest threats, tactics, and techniques used by cybercriminals.
- Collaboration with Law enforcement agencies: Collaboration with law enforcement agencies will help to track down the cybercriminals and bring them to justice.

In addition to implementing these measures, organizations should also stay informed about the latest cybersecurity trends and best practices and be prepared to adapt their security strategies as needed to stay ahead of emerging threats.
Cybersecurity refers to the protection of internet-connected systems, including hardware, software, and data, from attack, damage, or unauthorized access. Cybercrime, on the other hand, refers to criminal activity that uses or targets

internet-connected systems. Examples of cybercrime include hacking, identity theft, and the spread of malware. Effective cybersecurity involves using a combination of technologies, policies, and best practices to secure systems and protect against cybercrime. There are several cybersecurity challenges in protecting the digital environment, including:

- Advanced threats: Cyber criminals are becoming more sophisticated in their methods, making it increasingly difficult to detect and prevent attacks.
- Lack of security awareness: Many individuals and organizations lack the knowledge and training necessary to protect themselves from cyber threats.
- Complex and ever-changing technology: The rapid pace of technological change makes it difficult to keep up with new vulnerabilities and threats.
- Dependence on third-party vendors: Many organizations rely on third-party vendors for their IT infrastructure and services, creating additional security risks.
- Limited resources: Many organizations have limited resources and budget allocated to cybersecurity, making it difficult to implement adequate security measures.
- Insufficient regulations: Lack of standardization and uniform regulations makes it difficult to protect against cyber-attacks across industries and countries.
- IoT and connected devices: The increasing number of IoT devices connected to the internet creates new attack vectors for cyber criminals to exploit.

The rules and regulations surrounding cybercrime can vary depending on the jurisdiction and the specific type of crime. In general, however, there are several international, national, and state laws that address cybercrime. The Council of Europe's Convention on Cybercrime is the first international treaty on crimes committed via the Internet and other computer networks. It provides a framework for cooperation between nations in investigating and prosecuting cybercrime. The United States has several federal laws that address different types of cybercrime, such as the Computer Fraud and Abuse Act, which criminalizes unauthorized access to computers, and the Electronic Communications Privacy Act, which addresses illegal electronic surveillance. Many countries have their own national laws to address cybercrime, such as the United Kingdom's Computer Misuse Act. International organizations, such as Interpol and Europol, also play a role in investigating and combating cybercrime by facilitating cooperation between nations. It's also worth mentioning that many companies and organizations have their own cybersecurity protocols and policies to protect against cybercrime, such as incident response plans, security awareness training and penetration testing.

4. CONCLUSIONS

Cybersecurity is a significant matter as it has the ability to deal with the causes that threaten the security of information. However, cyberattacks pose a threat in different ways, and countermeasures must be implemented with awareness of the latest trends. As the methods of cyber-attacks are evolving day by day, it is always difficult to take comprehensive measures. Accordingly, this article contributed to presenting the most important practices and procedures that must be taken into account in their performance to protect the digital environment from cyber-attacks. Modern methods must be utilized to improve the mechanisms operated by companies while educating employees about the seriousness and threats of cyberspace. Applying international standards in enhancing the mechanisms of protecting the digital environment. Constant striving to provide specialized groups in cyber defense and cyber security against electronic attacks and cyber-crimes. Growing programs, applications, and computer systems to be able to face all types of cyber-attacks. All companies must have unique mechanisms in combating cyber-attacks by utilizing modern and advanced technologies based on artificial intelligence to create defenses against spying, data theft, and prevent entry to unauthorized individuals or malicious software. Finally, attention must be paid to the matter of cybersecurity and adapting to the modern and rapid growth of cyberspace through a comprehensive strategy for the prevention of cybercrime.

REFERENCES

[1] Button M., Shepherd D., Blackbourn D., Sugiura L., Kapend R., and Wang V., “Assessing the seriousness of cybercrime: The case of computer misuse crime in the United Kingdom and the victims’ perspective,” *Criminology & Criminal Justice*, pp:1-22, October 2022. https://doi.org/10.1177/17488958221128128

[2] Alawida M., Omolara A. E., Abiodun O. I., and Al-Rajab M., "A deeper look into cybersecurity issues in the wake of Covid-19: A survey," *Journal of King Saud University - Computer and Information Sciences*, vol.34, no.10, pp:8176-8206, November 2022. https://doi.org/10.1016/j.jksuci.2022.08.003

[3] Lubis M. and Handayani D. O. D., "The relationship of personal data protection towards internet addiction: Cyber crimes, pornography and reduced physical activity," *Procedia Computer Science*, vol.179, pp:151-161, 2022. https://doi.org/10.1016/j.procs.2021.12.129

[4] Arpaci I. and Aslan O., "Development of a Scale to Measure Cybercrime-Awareness on Social Media," *Journal of Computer Information Systems*, pp:1-11, July 2022. https://doi.org/10.1080/08874417.2022.2101160

[5] Mijwil M. M., Doshi R., Hiran K. K., Al-Mistarehi AH, and Gök M., "Cybersecurity Challenges in Smart Cities: An Overview and Future Prospects," *Mesopotamian journal of cybersecurity*, vol.2022, pp:1-4, 2022. https://doi.org/10.58496/MJCS/2022/001

[6] Navas-Camargo F. and Castro C. A. A., "Cyberspace, Artificial Intelligence, and the Domain of War. Ethical Challenges and the Guidelines Proposed by the Latin American Development Bank," In Security and Defence: Ethical and Legal Challenges in the Face of Current Conflicts, pp: 37–55, March 2022. https://doi.org/10.1007/978-3-030-95939-5_3

[7] Mijwil M. M., Sadıkoğlu E., Cengiz E., and Candan H., "Siber Güvenlikte Yapay Zekanın Rolü ve Önemi: Bir Derleme," *Veri Bilimi*, vol.5, no.2 pp:97-105, December 2022.

[8] Yang M. and Wang X., "Interaction Design of Wellness Building Space by Deep Learning and VR Technology in the Context of Internet of Things," *Wireless Communications and Mobile Computing*, vol.2022, no.6567431, pp:1-10, June 2022. https://doi.org/10.1155/2022/6567431

[9] Hu P., Chen W., He C., Li Y., and Ning H., "Software-Defined Edge Computing (SDEC): Principle, Open IoT System Architecture, Applications, and Challenges," *IEEE Internet of Things Journal*, vol.7, no.7, pp:5934 - 5945, July 2020. https://doi.org/10.1109/JIOT.2019.2954528

[10] Roopa M. S., Pattar S., Buyya R., Venugopal K. R., Iyengar S. S., and Patnaik L. M., "Social Internet of Things (SIoT): Foundations, thrust areas, systematic review and future directions," *Computer Communications*, vol.139, pp:32-57, May 2019. https://doi.org/10.1016/j.comcom.2019.03.009

[11] Tao F., Akhtar M. S., and Jiayuan Z., "The future of Artificial Intelligence in Cybersecurity: A Comprehensive Survey," *EAI Endorsed Transactions on Creative Technologies*, vol.8, no.28, pp:1-15, July 2021. https://doi.org/10.4108/eai.7-7-2021.170285

[12] Salem I. E., Salman A. M., and Mijwil M. M., "A Survey: Cryptographic Hash Functions for Digital Stamping," *Journal of Southwest Jiaotong University*, vol.54, no.6, pp.1-11, December 2019. https://doi.org/10.35741/issn.0258-2724.54.6.2.

[13] Salem I. E., Mijwil M. M., Abdulqader A. W., Ismaeel M. M., Alkhazraji A., and Alaabdin A. M. Z., "Introduction to The Data Mining Techniques in Cybersecurity," *Mesopotamian Journal of Cybersecurity*, vol.2022, pp:28-37, May 2022. https://doi.org/10.58496/MJCS/2022/004

[14] Why Upgrade to Data Security Firewall?, https://www.gajshield.com/index.php/why-data-security-firewall

[15] Ali A., "Cyberspace and Organized Crime: The New Challenges of the 21st Century," *International Journal of advanced humanities Research*, vol2, no.1, pp:22-37, January 2022. https://doi.org/10.21608/IJAHR.2022.256386

[16] Bayramova A., Edwards D. J., and Roberts C., "The Role of Blockchain Technology in Augmenting Supply Chain Resilience to Cybercrime," *Buildings*, vol.11, no.7, pp:1-19, June 2021. https://doi.org/10.3390/buildings11070283

[17] Monteith S., Bauer M., Alda M., Geddes J., Whybrow P. C., and Glenn T., "Increasing Cybercrime Since the Pandemic: Concerns for Psychiatry," *Current Psychiatry Reports*, vol. 23, no. 18, pp:1-9, March 2021. https://doi.org/10.1007/s11920-021-01228-w

[18] Al-Khater W. A., Al-Maadeed S., Ahmed A. A., Sadiq A. S., Khan M. K., "Comprehensive Review of Cybercrime Detection Techniques," *IEEE Access*, pp:137293 - 137311, July 2020. https://doi.org/10.1109/ACCESS.2020.3011259

[19] Narwal B., Mohapatra A. K., and Usmani K. A., "Towards a taxonomy of cyber threats against target applications," *Journal of Statistics and Management Systems*, vol.22, no.2, pp: 301-325, March 2019. https://doi.org/10.1080/09720510.2019.1580907

[20] Aggarwal, K., Mijwil, M. M., Sonia, Al-Mistarehi, AH., Alomari, S., Gök M., Alaabdin, A. M., and Abdulrhman, S. H., "Has the Future Started? The Current Growth of Artificial Intelligence, Machine Learning, and Deep Learning," *Iraqi Journal for Computer Science and Mathematics*, vol.3, no.1, pp:115-123, January 2022. https://doi.org/10.52866/ijcsm.2022.01.01.013

[21] Al Azzam S. B. N., "The AI algorithm for text encryption using Steganography," *Mesopotamian Journal of Cybersecurity*, vol.2020, pp:18-27, 2020. https://doi.org/10.58496/MJCS/2022/003

[22] Mijwil M. M., Salem I. E., and Ismaeel M. M., "The Significance of Machine Learning and Deep Learning Techniques in Cybersecurity: A Comprehensive Review," *Iraqi Journal For Computer Science and Mathematics*, vol.4, no.1, In press, January 2023. https://doi.org/10.52866/ijcsm.2023.01.01.008

[23] Mijwil M. M., Aggarwal K., Doshi R., Hiran K. K., and Gök M., "The Distinction between R-CNN and Fast R-CNN in Image Analysis: A Performance Comparison," *Asian Journal of Applied Sciences*, vol.10, no.5, pp:429-437, November 2022. https://doi.org/10.24203/ajas.v10i5.7064

[24] Muhammad T. and Ghafory H., "SQL Injection Attack Detection Using Machine Learning Algorithm," *Mesopotamian journal of cybersecurity*, vol.2022, pp:5-17, 2022. https://doi.org/10.58496/MJCS/2022/002

[25] Mustaffa S. N. F. N. B. and Farhan M., "Detection of False Data Injection Attack using Machine Learning approach," *Mesopotamian Journal of Cybersecurity*, vol. 2022, pp: 38–46, July 2022. https://doi.org/10.58496/MJCS/2022/005

[26] Mijwil M. M., Filali Y., Aljanabi M., Bounabi M., Al-Shahwani H., and ChatGpt "The Purpose of Cybersecurity in the Digital Transformation of Public Services and Protecting the Digital Environment," *Mesopotamian journal of cybersecurity*, vol.2022, pp:1-5, 2022.

[27] Alwan A. H. and Kashmar A. H., "FCNN Model for Diagnosis and Analysis of Symmetric Key Cryptosystem," *Iraqi Journal For Computer Science and Mathematics*, vol. 4, no. 1, pp. 53–61, November 2022. https://doi.org/10.52866/ijcsm.2023.01.01.006

[28] Mijwil, M. M., "Malware Detection in Android OS Using Machine Learning Techniques," *Data Science and Applications*, vol.3, no.2, pp:5-9, 31 December 2020.

[29] Mutar D. S., "Computer Network Attack Detection Using Enhanced Clustering Technologies," *Asian Journal of Applied Sciences*, vol. 9, no.6, pp:392-396, December 2021. https://doi.org/10.24203/ajas.v9i6.6839

[30] Alajanbi M., Ismail M. A., Hasan R. A., and Sulaiman J., "Intrusion Detection: A Review," *Mesopotamian Journal of Cybersecurity*, vol.2021, pp:1-4, January 2021. https://doi.org/10.58496/MJCS/2021/001

[31] Aljanabi, M. ., Mohanad Ghazi, Ahmed Hussein Ali, Saad Abas Abed, & ChatGpt. (2023). ChatGpt: Open Possibilities. Iraqi Journal For Computer Science and Mathematics, 4(1), 62–64. https://doi.org/10.52866/ijcsm.2023.01.01.0018