ISSN: 2037-4445

Cyber Security As A New Strategic Issue in the Middle East: A Case Study of Persian Gulf and North African Countries

Ellias Aghili Dehnavi[1], Radosław Arkady Fiedler*[2]

Abstract

In this paper, cyber security as a new strategy in the countries of the Persian Gulf and North Africa has been investigated. In this regard, the most important cyber-attacks carried out in these areas have been identified and classified. Accordingly, Phishing, Denial of service, Man-in-the-middle, Day-Zero and Backdoors have been identified as the most dangerous cyber-attacks in these areas. The impact of social media and the Internet on Islamic awakening, the attack of the Stuxnet virus to counter Iran's cyber capabilities through cooperation with the countries of the Persian Gulf can be considered as one of the most important reasons for the attention of the countries of the Persian Gulf to cyber security. In addition, China, Russia, and the United States have had the greatest foreign influence and intervention in cyber security in the Middle East. Among North African countries, Tunisia can be considered the most advanced country in the field of cyber security. Legislation, standards and policy and training of end users can be considered the most important actions of North African countries to deal with threats and cyber-attacks. While in the Persian Gulf countries, cyber surveillance of non-state actors and cyber laws are the most important actions taken.

Keywords: Cyber-attacks, cyber security, Persian Gulf, Middle East, North Africa.

1. Introduction

According to the Global Economic Crime Report in 2016, cybercrime is one of the biggest economic crimes in the Middle East, which affected 30% of organizations this year [1]. The reason for the increase in these crimes is the decision of the Arab Gulf Cooperation Council (GCC) to reduce dependence on the oil and gas industry through the creation of a strategic development framework, with the aim of creating new economies for the future of this council's members [2]. However, it has become clear that this strategic framework is increasingly under threat due to insufficient advances in cyber security strategies.

The GCC development framework mainly includes the development of digital technology, the use of intelligent IoT infrastructure and technology for the growth of the digital economy. Smart cities are able to significantly change economic and social structures and be widely economically beneficial [3]. Cybercrime poses a multifaceted threat to security in the Middle East. The reason is that many components of these infrastructures are accessible and this increases the rate of security threats. Another reason for this is the use of personal devices by employees at work. Lack of regulations and poor security awareness have exposed more than 65% of employees to security risks. As a result, businesses are increasingly being targeted by cybercriminals across the region [4].

Cybersecurity is a term first used by William Gibson in 1962. Cybersecurity is the set of processes, technologies, and practices defined in terms of how they are designed to help protect various applications, devices, networks, and data from malicious attacks that gain unauthorized access and damage to these resources [5].

In this definition, cyberspace refers to networks that are connected through information highways such as the Internet, and all information about the relationships of people, cultures, nations, countries, and in general everything that exists on the earth in a physical and tangible form, exists in digital form and

[1] Ph.D. Student in Regional studies (Middle East and Northern African countries), department of International Relations, faculty of law and political sciences, Allameh Tabataba'i university, aghili_el97@atu.ac.ir

[2] Supervisor author, Professor of International relations, head of the Department for Non-European Political Studies at the Faculty of Political Science and Journalism, Adam Mickiewicz University, Poznan, Poland, radoslaw.fiedler@amu.edu.pl

can be used and accessed by users, and it is connected through computers, its components and international networks [6].

As the volume and complexity of Internet technology and mobile applications increase, malicious cyber-attacks are evolving, and as a result, society faces more cyber security risks than ever before [7]. To protect the organization's critical data and information system assets, organizations have deployed sophisticated monitoring systems such as password management, data intrusion prevention and content monitoring technologies, as well as security technologies such as firewalls for perimeter defence.

Cyber-crimes are mainly aimed at wealthy economies. The prosperity of the oil-based economies of the Persian Gulf Cooperation Council, which is accompanied by digitalization, has made the Middle East region an attractive target for cybercrimes [8]. In Saudi Arabia, between 2000 and 2009, Internet usage increased 30 times. About 23% of users have been victims of cyber-crimes.

In the UAE, 76% of Internet users have fallen victim to cybercriminals, and as a result of these crimes, about 630 million dollars have been damaged to the country's economy [9]. The number of reported cases of cyber-crimes in other GCC countries is as follows: 95,000 cases were reported in Kuwait, 60,000 cases in Bahrain and 37,000 cases in Oman. Also, more than 2,871 cybercrime-related arrests were made in Qatar in one year [10].

Cybercrime related to cellular devices is also on the rise because the penetration rate of such devices in the economy is high. In North African countries, more than 20% of cyber-attacks are carried out through mobile internet in this region. This should be considered with the increase in mobile transactions and the rapid rise of mobile malware.

In such a condition, cyber security has become a strategic strategy in the Middle East region, especially in North African countries and the oil-rich countries of the Persian Gulf. It is necessary and important to examine its various dimensions.

2. Types of cyber-attacks in the Middle East and North Africa

There are different types of electronic attacks, some of which are as follows:

1) Phishing

It is a method that often relies on social engineering. Hackers encourage their victim to open the infected malware link. Once the person opens the message, the hacker begins the theft process through emails, private messages or even apps installed on social media sites that are now vulnerable to such threats and attacks [11].

2) Denial of service

This is a dangerous form of electronic attack. The attack starts with a computer program designed to control many computers and create robotic networks between them, known as botnets. These botnets are used by hackers to carry out denial of service attacks. Controlled networks flood the victim's computer system with numerous messages and requests, which eventually disrupts the essential services of even a website [12].

3) Man-in-the-middle

This happens when the hacker places himself in the communication transmission channel between the sender and the receiver. In this attack, the hacker changes the client's IP address. Hence, users will continue to believe that they are in contact with the right person. IP spoofing, which is a form of this attack, is used by the hacker to convince any system that it is connected to a known and trusted entity, thereby giving the attacker access to the system [13].

4) Day-Zero

The attack refers to intrusions into smartphones, computer applications, and operating systems that are not yet known to security researchers and developers [14].

5) Backdoors

Most of them are well-known vulnerabilities, but they are usually intended to be created by organizations or companies to get directly into the user's device to help fix some technical problem.

Backdoors are often difficult to detect, and detection methods often differ depending on the operating system used by the computer [15].

3. The reasons for the attention of Persian Gulf countries to cyber security

Three key events caused the Persian Gulf countries to pay attention to cyber security.

1) The first event was the impact of social media and the Internet on the Islamic awakening of 2011 [16].

2) The second event was the Stuxnet virus attack.

3) The third reason was that in response to Iran's ever-increasing cyber capabilities, America has started cooperation with the Persian Gulf countries to improve their cyber defense capabilities.

4. Iran, a pioneer in the field of strengthening cyber security in the Middle East region

Iran's superiority in the field of cyber over the Persian Gulf countries is considerable. The use of cyber techniques as a tool of national power has become a rule in the Persian Gulf. The Persian Gulf is unparalleled in the use of cyber techniques. The development of cyber capabilities in Iran is very prominent among them. Iran has used this technique and is ready to use it again. The use of cyber tools and the development of cyber capabilities can change the balance of military forces among countries in the region [17].

Iran's trajectory in developing cyber capabilities is a good example. The Persian Gulf countries are also strengthening their defence capabilities in response to Iran's increasing cyber capabilities. Qatar, Saudi Arabia and Bahrain have launched their cyber security programs. Kuwait also has a 1-billion-dollar program in the field of cyber security with the cooperation of the UK. The variables that determine the probability of cyber-attacks in the future are the type of relations between Iran, its neighbours and foreign players, the probability of attacks and the quality of cyber defence of the Persian Gulf countries [18].

5. Cyber threat against Persian Gulf countries

The director general of the Saudi National Cyber Security Center has announced that all member countries of the Persian Gulf Cooperation Council are facing the threat of these attacks. In fact, cyber-attacks on member countries of the Gulf Cooperation Organization (Persian Gulf) are increasing day by day. Bahrain has also announced that hackers have repeatedly tried to disrupt computer systems related to government institutions in the country. In addition, the Central Information Technology Agency of Kuwait has also announced that the country's economic institutions were also subjected to cyber-attacks. Many cyber-attacks have been carried out in the Persian Gulf countries against the oil companies of this region.

Most of the attacks that take place do not become media, and if smart cities expand, anything can be achieved. According to the report of Kaspersky, only in the first quarter of 2016, 2.2 billion cyber-attacks occurred in the whole world. According to this report, in the Middle East, countries such as Egypt, Turkey and Qatar are the target of the most cyber-attacks and Lebanon is known as the safest country in terms of the amount of cyber-attacks. The number of ransomware has also experienced a 15% growth in this region, and most attacks have occurred through emails, social networks, websites, routers, and external memory devices or USB. Also, 17% of attacks occurred on Android devices, 61% through browsers, 11% through Java, 4% through Microsoft Office, and 3% through Adobe Reader. Therefore, cyber-attacks and security related to this area are considered a new issue and crisis for the Persian Gulf countries.

Predicting the state of attacks and cybercrimes in the Persian Gulf countries and North Africa

Predictions indicate that the Middle East region, especially the Persian Gulf countries, will continue to be the target of cyber-criminal activities in 2023. In addition, these surveys show that a third of users in the Middle East and North Africa region were affected by online and offline threats between January and September 2022. Cyber security companies have predicted that this year there is a possibility of a new large-scale malicious digital attack, and one of the possible reasons for that is the exploitation of existing weaknesses by one of the most developed and powerful malicious entities, especially as current global tensions increase the opportunity for cyber threats. These cyber security networks have reported the possibility of malicious attacks affecting the government sector and other main sectors, some of which are not easily traceable [19].

6. The impact of foreign interventions on cyber security in the Middle East

Russia's support for the Assad regime will likely be accompanied by increased surveillance and cyber defence regime. The investment of Chinese companies in the field of artificial intelligence in the Persian Gulf and the sale of drones by them to the Persian Gulf countries is also significant. Due to Russia's and China's expanding approaches, growing technology and their cyber interests in the Middle East, authoritarian cyber security and cyber espionage are expected to strengthen in the region, especially in the energy sector. China's recent cyber deals with Iran may also push other countries in the region to cooperate with the United States. China and Russia, as the main supporters of Iran's cyber capabilities, can turn this country into a cyber-security giant in the region. The United States is interested in working with regional governments in the cyber domain to secure the flow of energy and international trade. In this way, it should share its expertise in the field of cyber defence with its partners in the region. On the other hand, the cyber interference of the United States in the region can lead to reactions from Iran in relation to Israel and the United States. After the Stuxnet attack, Iran has developed considerable cyber capabilities. The United States should not become directly involved in a cyber-war in the region and can continue its current level of involvement in cyber defence, intelligence sharing, and research and development. Facebook and Instagram are the most influential because of their role in content creation and this trend is expected to continue in the next five years [20].

7. The progress of cyber security forces in the countries of the Persian Gulf and North Africa

A cyber security company called Darkmatter is founded in Abu Dhabi. The company began hiring new staff in late 2014 and has since nearly tripled its workforce to 650. Darkmatter hired executives from major international companies such as Intel and Blackberry, some of whom had experience in Western intelligence and military organizations, including the US National Security Agency (NSA).

A large part of the activities carried out in the Persian Gulf countries with government agencies is related to how to strengthen networks for safety and immunity from cyber-attacks or recovery after attacks because cyber-attacks by adversaries, militant groups, or cyber criminals can damage key infrastructure such as oil and gas facilities and desalination plants that many other Gulf countries depend on. The United Arab Emirates recorded the lowest number of non-internet-related electronic threats in the region; which are made through connected peripheral devices such as USB devices, SP, various disks or wired connections.

Saudi Arabia and the United Arab Emirates are competing for the top spot in the region's cyber security and espionage and hacking tools. Saudi Arabia's efforts to develop its cyber capabilities are bearing fruit, while domestic business opportunities for the UAE are shrinking. Determined to play a regional role, Saudi Arabia uses both soft and hard power to increase its absorption of the latest technologies. The trade fairs, which symbolize the battle and cyber competition for influence among the Gulf states, are one aspect of the soft power strategy that Saudi Arabia is using to balance its cyber competition with the UAE. Saudi Arabia's late entry into the cyber sector has been accompanied by massive investments by the country's public funds, particularly the Public Investment Fund [21]. Qatar is also trying not to ignore the issue of cyber-attacks in commercial infrastructure and is trying to develop its cyber domain internet and espionage tools. The responsibility for this was partly put in the hands of Haboob, a company founded in 2018 that recruited the best hackers of the royal court to improve cyber security.

Egypt and most North African countries are also developing their cyber capabilities and have been able to neutralize many cyber-attacks with timely control.

8. Cyber security initiatives in North Africa

Egypt and Morocco are among the African countries that have the highest Internet traffic. Algeria and Tunisia also have the next ranks in this regard. Therefore, these countries are also pioneers in the field of implementing cyber security plans. Tunisia has a computer emergency response team consisting of individuals with advanced degrees in information security. In fact, this country can be considered the most advanced country in the North African region in the field of cyber security. Tunisia's National Security Intelligence Agency has made the implementation of cyber security plans mandatory in this country by passing the law. Also, various organizations have been established in North African countries, including Tunisia, which train information and communication technology specialists and are thus trying to improve cyber security awareness and capabilities throughout Tunisia [22].

In North Africa, only Egypt has formal laws against cybercrime, while Morocco has laws in place. No initiatives are visible in Libya or other countries in the region. In particular, Egypt has tried to strengthen its position in the global economy as a reliable source by implementing cyber security initiatives. Also, the Egyptian government has complete control over all activities carried out in the field of cyber security. Any violation of the requirements and laws in this regard will also face heavy financial penalties from the government of this country. Repetition of violations will result in multiple penalties for the violators. Morocco and Sudan have also shown interest in implementing cyber security plans by participating in the regional conference in Casablanca and by planning meetings to develop cyber security laws. The most important initiatives used by North African countries in the field of cyber security are shown in table (1) [22].

Table (1): The most important initiatives used by North African countries in the field of cyber security

Country	Training of end users	Law of computer crimes	Standards and policies	Expressing the desire to implement cyber security plans	Validation	PKI	Law enforcement	Identity theft	Legislation	High level of education	CERT/CSIRT
Tunisia											
Algeria											
Egypt											
Morocco											
Sudan											
Libya											

9. Cyber security initiatives in Persian Gulf states

Most countries in the Middle East are trying to improve their security against cyber-attacks. Some are also building the capacity to carry out cyber-attacks as a defensive and preventive tool.

9. 1. Cyber surveillance of non-state actors

Israel, with its efforts in the field of gathering signal information and code decoding, is considered a good example of a cyber-defence process. In addition, cyber defence may also include cyber-attacks. Israel is taking preventive steps against Iran with the aim of neutralizing the country's offensive capability. Some Persian Gulf countries such as Saudi Arabia also cooperate with Israel for this purpose. Iran is also creating and growing its cyber forces. Considering that Iran is under the influence of international sanctions, it is under pressure to strengthen its cyber programs. Although Iran's cyber security program is less advanced than the United States, Israel, Britain, China, and Russia, these programs are growing and strengthening [23].

Many countries in the Middle East have cyber surveillance programs and units that are in the early stages of development. For example, there are reports of a cyber-group in Egypt claiming that the purpose of the country's cyber security programs is to defend Egypt's critical infrastructure against terrorist attacks. The purpose of this group is to deal with non-state actors. Such actors are a major source of instability in the Middle East and pose security challenges previously seen only among state actors.

Another cyber unit formed in the Persian Gulf is the Qatar Electronic Army, which consists of Internet hackers supporting the Qatari government. They specifically target dissident groups and use attacks such as hacking websites and altering content.

9. 2. Cyber laws

Legislation is an integral part of combating global cyber threats. Cyber laws in the Middle East are either in their early stages or under active development in most countries. Legislators in the Persian Gulf countries deal with issues related to cybercrimes by applying judicial measures including criminal, regulatory and civil laws. Setting more laws to deal with cybercrime may be more effective.

The countries of Jordan, Oman, Saudi Arabia and the UAE have taken important measures in the field of cybercrime and cyber security laws. The federal law of the UAE under the title of fighting against cybercrimes is one of the important actions of this country in the field of cyber security. According to this law, if a person uses a computer network or social media to violate the privacy of other people, or if the legal institutions consider it an insult or harassment to a person, he/she can be imprisoned for 6 months or fined [23].

Saudi Arabia also has a cybercrime law that aims to improve cyber security by identifying crimes and determining penalties to protect "information security, protect rights related to the legitimate use of computers and information networks." In this regard, punishments for cyber-crimes such as identity theft, defamation, etc. have been considered.

Oman has passed laws to fight cybercrimes and promote cyber security in the country. This law identifies a wide range of illegal activities and, depending on the severity of the crime, provides punishments ranging from fines to imprisonment for the violators. Jordan also has an Information Systems and Cybercrimes Act that covers the full range of cybercrimes, including minor offenses such as unauthorized access to computer content to more serious offenses such as identity theft and credit card fraud [23].

Also, some countries in the Middle East have begun to understand the importance of protecting people's personal information. Egypt, Israel, Saudi Arabia and UAE are among these countries.

10. Stages of cyber security in the countries of the Persian Gulf and North Africa

10. 1. Prevention

This stage includes identifying the ways of penetration and attack and dealing with it to increase the security, safety and stability factor [24]. The following are among the most important methods of cybercrime prevention:

1) The stable design of systems

If security is included among the criteria and principles of system design, the systems will be much safer and more stable than before.

2) Stopping the attacks

Stopping attacks is another way to prevent attacks. This is possible through the use of advanced security equipment and the establishment of appropriate laws.

10. 2. Incident management and damage limitation

The methods of managing accidents and limiting the harmful effects of accidents are the methods that can be used to reduce the effect of attacks in the shortest possible time.

1) Determining signs, symptoms and warnings

This means that when an attack is carried out, the effects and potential dangers of this attack must be identified first, because by identifying the effects of an attack, the consequences of other attacks and the dangers that may arise can be prevented.

2) Securing and stabilizing systems

To prevent external influences, it is necessary to create barriers. One of the oldest barriers to penetration is the use of passwords, and newer methods are the use of methods such as firewalls and proxy servers. Any of these failures may lead to failure. In the case of physical attacks, it is necessary to identify all possible attacks and intrusions. For example, in the case of an information network, appropriate physical strategies should be adopted to make its data centers safe, secure and stable.

3) shutdown and reallocation

Another solution is to completely or partially shut down the system and reallocate it. A system that realizes that it is under an attack must build barriers and defences that it may not use in normal situations and try to isolate the parts of the system that are under attack. Of course, the shutdown and reassignment steps must be done in real time and quickly.

10. 3. Support

The noteworthy point is that the collected information should always be supported before any attack. This tactic is achieved through the preparation of the information backup version. Many defence methods need to know the correct state of the system before the attack to facilitate recovery and redesign. This method is for times when attacks are carried out based on a precise starting point and supports are regularly stored. Many attacks are slow and stealthy, causing more problems than when the information was intact. In this case, in order to create a healthy environment, the organization's systems must have their own programs to prepare the backup version.

11. The future of cyber security in the Middle East and North Africa

Future cyber-attacks consist of pre-programmed independent tools that are designed to infect organizational networks and can steal information or destroy organizations' data in just a few minutes. However, despite the fact that countries in the region have made extensive investments to prepare themselves for any cyber-attack, hackers are still a few steps ahead, and therefore it cannot be said that no cyber-attack will occur. The experts of Research and Markets Center recommended that in order to be more secure, all cyber security activities should be integrated in a central agency so that a country can take steps in this field better than ever before. In many countries, it is still seen that government organizations and private agencies each use a separate security tool and each of them take separate steps to deal with cyber-attacks, which cannot strengthen them. The Middle East is taking steps towards making its cities smarter, and this issue will also have an impact on strengthening the security of the cyberspace as much as possible.

12. Conclusion

The most dangerous cyber-attacks detected in the countries of the Persian Gulf and North Africa are Phishing, Denial of service, Man-in-the-middle, Day-Zero and Backdoors. The impact of social media and the Internet on Islamic awakening, the attack of the Stuxnet virus to counter Iran's cyber capabilities through cooperation with the countries of the Persian Gulf can be considered as one of the most important reasons for the attention of the countries of the Persian Gulf to cyber security. Among the countries of the Middle East, Iran has progressed more than other countries in the field of cyber security, and one of the most important reasons has been the country's confrontation with Israeli cyber-attacks. Also, the prediction of the future situation of cyber-attacks and crimes in the countries of the Persian Gulf and North Africa indicates the continuation and intensity of these attacks in the coming years. In addition, China, Russia, and the United States have had the greatest foreign influence and intervention in cyber security in the Middle East. Among North African countries, Tunisia can be considered the most advanced country in the field of cyber security. Also, Egypt is the only country with formal laws against cybercrime, while Morocco has laws in place, but no initiatives are visible in Libya or other countries in the region. Legislation, standards and policy and training of end users can be considered the most important actions of North African countries to deal with threats and cyber-attacks. While in the Persian Gulf countries, cyber surveillance of non-state actors and cyber laws are the most important actions taken. The stages of cyber security in the countries of the Persian Gulf and North Africa include prevention, incident management and limiting failures and support. Persian Gulf countries and some North African countries such as Tunisia have taken effective steps in improving cyber security. Nevertheless, these measures were not enough, especially in the case of the Persian Gulf countries, which are facing numerous threats and cyber-attacks in the oil and energy field.

Using more advanced technologies and methods and investing more in this field can minimize the damage caused by cyber-attacks in these countries.

References

[1] El-Guindy, M. N. (2008). Cybercrime in the Middle East. *ISSA Journal*, *6*(6).

[2] Alshabib, H. N., & Martins, J. T. (2021). Cybersecurity: Perceived Threats and Policy Responses in the Gulf Cooperation Council. *IEEE Transactions on Engineering Management*, *69*(6), 3664-3675.

[3] Hassib, B., & Shires, J. (2022). Cybersecurity in the GCC: From Economic Development to Geopolitical Controversy. *Middle East Policy*, *29*(1), 90-103.

[4] Teoh, C. S., & Mahmood, A. K. (2018). Cybersecurity workforce development for digital economy. *The Educational Review, USA*, *2*(1), 136-146.

[5] Bay, M. (2016). What is cybersecurity? *French Journal for Media Research*, *6*, 1-28.

[6] Kostopoulos, G. (2017). *Cyberspace and cybersecurity*. Auerbach Publications.

[7] Cebula, J. L., & Young, L. R. (2010). *A taxonomy of operational cyber security risks*. Carnegie-Mellon Univ Pittsburgh Pa Software Engineering Inst.

[8] Williams, C. M., Chaturvedi, R., & Chakravarthy, K. (2020). Cybersecurity risks in a pandemic. *Journal of medical Internet research*, *22*(9), e23692.

[9] Al Neaimi, A., Ranginya, T., & Lutaaya, P. (2015). A framework for effectiveness of cyber security defenses, a case of the United Arab Emirates (UAE). *International Journal of Cyber-Security and Digital Forensics*, *4*(1), 290-301.

[10] Brown, R. D. (2018). Towards a Qatar Cybersecurity Capability Maturity Model with a Legislative Framework. *International Review of Law*.

[11] Qabajeh, I., Thabtah, F., & Chiclana, F. (2018). A recent review of conventional vs. automated cybersecurity anti-phishing techniques. *Computer Science Review*, *29*, 44-55.

[12] Aldhyani, T. H., & Alkahtani, H. (2023). Cyber Security for Detecting Distributed Denial of Service Attacks in Agriculture 4.0: Deep Learning Model. *Mathematics*, *11*(1), 233.

[13] Natarajan, J. (2020). Cyber secure man-in-the-middle attack intrusion detection using machine learning algorithms. In *AI and Big Data's Potential for Disruptive Innovation* (pp. 291-316). IGI global.

[14] Alhayani, B., Abbas, S. T., Khutar, D. Z., & Mohammed, H. J. (2021). Best ways computation intelligent of face cyber attacks. *Mater. Today Proc*, 26-31.

[15] Gold, S. (2014). Backdoors to the future?[communications cyber security]. *Engineering & Technology*, *9*(9), 59-63.

[16] Assoudeh, M. (2020). *Shaping Cybersecurity Strategy: China, Iran, and Russia in a Comparative Perspective* (Doctoral dissertation, University of Nevada, Reno).

[17] Bahgat, G. (2020). Iran and Its Neighbors Face Risks and Opportunities in Cyber Security.

[18] Abu-Taieh, E., Alfaries, A., Al-Otaibi, S., & Aldehim, G. (2018). Cyber security crime and punishment: comparative study of the laws of Jordan, Kuwait, Qatar, Oman, and Saudi Arabia. *International Journal of Cyber Warfare and Terrorism (IJCWT)*, *8*(3), 46-59.

[19] Alshabib, H. N., & Martins, J. T. (2021). Cybersecurity: Perceived Threats and Policy Responses in the Gulf Cooperation Council. *IEEE Transactions on Engineering Management*, *69*(6), 3664-3675.

[20] Shires, J. (2022). *The Politics of Cybersecurity in the Middle East*. Oxford University Press.

[21] Kshetri, N., & Kshetri, N. (2013). Cybercrime and cybersecurity in the Middle East and North African economies. *Cybercrime and Cybersecurity in the Global South*, 119-134.

[22] Cole, K., Chetty, M., LaRosa, C., Rietta, F., Schmitt, D. K., Goodman, S. E., & Atlanta, G. A. (2008). Cybersecurity in africa: An assessment. *Atlanta, Georgia, Sam Nunn School of International Affairs, Georgia Institute of Technology*.

[23] Aboul-Enein, S. (2017). Cybersecurity challenges in the Middle East. *GCSP*, *17*, 5-49.

[24] Ahmed, N. N., & Nanath, K. (2021). Exploring cybersecurity ecosystem in the middle east: Towards an SME recommender system. *Journal of Cyber Security and Mobility*, 511-536.