journal Of Legal and Economic Studies ISSN 2602-7321/ EISSN 2773- 2649
Vol : 05 No: 03 Year: 2023 Page : 1160 - 1173

Mechanisms for Achieving Cybersecurity in the Face of Contemporary Changes

Nabil nouis* [1], University Center of Barika, Algeria, nabil.nouis@cu-barika.dz

Alaeddine youcefi [2], University Center of Barika, Algeria, alaeddine.youcefi@cu-barika.dz

Send Article Date: 12 /06/2023 Date of acceptance of the article: 14/06/2023

Abstract:

The interest in achieving cyber security has become a priority for every country globally because of its importance in preserving information and data from theft and piracy and addressing various electronic terrorism. To achieve cyber security, we must adopt mixed technical, educational, media, and legislative mechanisms and methods, anti-virus techniques, and programs for e-mail and official accounts capable of addressing electronic attacks. The inclusion of anti-cybercrime systems within the educational curricula for all academic levels will enhance. The culture of digital security and enactment of accurate and comprehensive legislation that suits will the resistance to cyber-attacks through the formulation of laws that regulate and will keep pace with technological progress and the continuous cooperation between individuals and the security services of each country, as well as cooperation between countries to monitor and track hacking and information piracy.

key words: mechanisms, protection, cyber security, contemporary changes

Introduction:

The use of information technology has become necessary in various fields in our current era, which has brought people closer together and fulfilled their needs rapidly through these information devices and various communication tools. However, this has not prevented the emergence of certain problems that threaten the interests of individuals and countries when using computer equipment, the internet, and various communication devices. This includes the emergence of what is known as cyber-attacks and electronic threats executed by cybercriminals to gain access to information, steal it, or exploit it for espionage, terrorism, and other objectives they seek.

*nabil nouis.

Achieving cybersecurity has become a priority for nations to protect networks, software, devices, and data from attacks, hacking, sabotage, and network destruction. This requires adopting different methods to prevent these cyber threats and effectively respond to any network breaches promptly. In this discussion, we will focus on the methods of achieving cybersecurity and preventing electronic attacks and threats.

THE FIRST TOPIC: THE CONCEPT OF CYBERSECURITY

The term cybersecurity, derived from the Latin word "cyber" meaning the information space, refers to the comprehensive expression of the virtual world that encompasses everything related to the uses, mechanisms, applications, and equipment of information technology and computers, as well as the interconnection between them through computer networks, communications, and the internet.[1]

Cybersecurity is "a combination of technical, organizational, and administrative measures used to prevent unauthorized use, misuse, and recovery of electronic information, communication systems, and data while enhancing the protection, confidentiality, and privacy of personal data, and taking all necessary measures to protect citizens and consumers from risks in cyberspace."[2]

Edward Amoroso defines cybersecurity as "the means to reduce the risk of attacking software, computers, or networks," including tools used to combat hacking, detect and stop viruses, and provide encrypted communications.[3]

According to the International Telecommunication Union (ITU) in its report on "Reform in Telecommunications for 2010-2011," cybersecurity is "a set of missions, means, security policies, guidelines, risk management approaches, training, practices, and techniques that can be used to protect the cyberspace environment, institutional assets, and users."[4]

Joseph S. Nye identifies three types of actors who possess cyber power:

- States: States have significant capabilities to carry out cyber-attacks, develop infrastructure, and exercise authority within their borders.[5]

[1] Muhammad Al-Amin Al-Bashiri. Investigation of Computer Crimes. A research paper submitted to the Law, Computer, and Internet Conference held from May 1st to 3rd at the Faculty of Sharia and Law in the United Arab Emirates, 2000, p. 39.

[2] Mona Al-Ashqar Jubour. Cybersecurity: Challenges and Countermeasures. Arab Center for Legal and Judicial Research, 2012, p. 16.

[3] Awad Majid Ghaleb Al-Awadi. Cybersecurity: Information Security. Bayan Center for Studies and Planning, Beirut, 2016, p. 6

[4] ITU , Cybersecurity, Géneva : internationaltélécummunication Union (ITU),2008. P 125.

[5] Joseph .s Nye : JR ; Cyberpower , Harvard Kennedy School,2010. P 11.

- Non-State Actors: These actors primarily use cyber power for offensive purposes. However, their ability to execute impactful cyber-attacks requires the involvement and assistance of advanced intelligence agencies. Nonetheless, they can infiltrate websites and target defense systems.
- Individuals (Hackers): Individuals who possess high technical knowledge and the ability to employ it. They are often difficult to identify and track due to the anonymity associated with their activities.[1]

THE SECOND TOPIC: CYBER THREATS

The topic includes an introduction that deals with the points that are presented within it according to the division into Requirement

FIRST REQUIREMENT: DEFINITION

Cyber threats involve the exploitation of computers and information technology to sabotage and destroy opponents' information infrastructure. They can even disable air defense networks and infiltrate the email systems of heads of state for systematic espionage.

Cyber threats, or cyber-attacks, pose a risk to societal security, national economic security, and the military and defense aspects of nations. They target both the moral and material aspects on all levels.

Securing computer systems and information technology is vital to maintain the privacy, integrity, and availability of individuals' and organizations' actions. Without it, trust in sectors that rely on data processing and information exchange collapses. This can lead to individual or organizational paralysis or result in catastrophic consequences that are difficult to remediate, both financially and morally.

SECOND REQUIREMENT: KEY CYBER THREATS

Various forms of cyber threats differ in terms of sources and objectives, such as espionage and information theft. They can be summarized as follows:

Electronic Espionage: Electronic espionage is carried out using advanced technological means. Cyber-attacks in this context aim to obtain secret information through illegitimate methods. Cyber espionage relies on the use of electronic technologies to gather information. It varies in terms of types, including

[1] Hassan bin Ahmed Al-Shahri. Developed digital electronic systems for preserving and protecting the confidentiality of information from espionage." Noor Research Center for Electronic Research, 2010, p. 11.

individual-based espionage, wired network espionage, or even satellite-based espionage.[1]

Cybercrime: Cybercrime has significantly increased due to the development of communication technology and the rise of digital globalization. Although the Internet facilitates various economic and social activities, it also poses a range of risks, including data theft and unauthorized access to personal information[2]. Cybercrime refers to violations committed against individuals or groups to harm the victim's reputation, either physically or mentally, directly or indirectly, using communication networks such as the internet (e.g., chat rooms, email, and mobile phones). Computer-related activities for personal gain, financial harm, or damage, including identity-related crimes and acts related to computer content, all fall under cybercrime.[3]

The most significant cybercrimes are:

- Information security, including its credibility, availability, and integrity. This includes activities such as system breaches through password theft, phishing, deception, fraud, and data destruction and theft.
- Personal safety, such as stalking and surveillance of children with the intent to harm or exploit them sexually. This category also includes activities like luring individuals for human trafficking, organ trade, production, or distribution of pornography.
- Financial aspects, involving fraud, forgery, extortion, and money laundering.
- Content-related crimes, such as distributing child pornography, spreading hate speech, promoting mercenary services, or advocating terrorism.
- National security and sovereignty, including activities like espionage and disclosure of classified information.
- Intellectual property, encompassing software theft, piracy, and unauthorized use of intellectual property-protected creations.[4]

Cyber Terrorism: Cyberterrorism refers to the use of information resources, including media, computers, the internet, and satellites, for the purpose of intimidation, coercion, political manipulation, negative ideological persuasion, and aggression. Cyberterrorism can paralyze command, control, and communication

[1] Amjad Al-Munif. Electronic Terrorism - A Modern Battle." Arab Magazine, Issue 7, July 2015, p. 02.

[2] Amira Muhammad Muhammad Sayed Ahmed. Strategies for Combating Cybercrimes in the Information Age." Journal of Media Research, Faculty of Media, Al-Azhar University, Issue 58, Part Four, Cairo, 2021, p. 178.

[3] Idris bin Tayeb Atiya. The Phenomenon of Terrorism in the Post-Modern Era: An Analytical Study of Forms, Methods, and Countermeasures." Arab Journal of Security Studies and Training, Volume 31, Issue 63, Riyadh, 2015, p. 24.

[4] Mona Al-Ashqar Jubour. Siberania: The Obsession of the Era." Arab Center for Legal and Judicial Research, Beirut, 2017, p. 50.

systems, and disrupt communication networks, central units, and air defense systems.[1]

Cyber Warfare: Cyber warfare relies on a team of experts in electronic battles, each with their own responsibilities and specialized skills to establish and control combat capabilities within cyberspace. Cyber warfare operators plan, manage, and execute offensive and defensive activities through cyberspace.[2]

THIRD REQUIREMENT: CYBER THREAT PATTERNS

Cyber threats faced by nations and individuals can be classified into four main patterns:

- Denial of Service (DoS) Attacks: In this pattern, a large volume of requests and tasks is launched at the victim's servers in a way that exceeds their processing capacity, causing partial or complete interruption or slowdown of their operation. This type of attack is frequently used against websites, banks, or institutions to impact their functionality or demand financial ransom.[3]
- Information Destruction or Modification: This refers to unauthorized access to the victim's information through the internet or private networks and altering important data without the victim's knowledge. The data remains present but is misleading, potentially leading to catastrophic outcomes, especially if it involves military plans, schedules, or classified maps.[4]
- Network Espionage: This involves unauthorized access and spying on an adversary's networks without destroying or altering the data. The goal is to obtain sensitive information, which may include military, economic, financial, or political secrets, negatively impacting the adversary's operations.
- Information Destruction: In this case, there is complete wiping out and destruction of assets, information, and data present on the network. This is commonly referred to as a "content safety threat" and involves making changes in data, either through deletion or destruction, by unauthorized individuals.[5]

Based on the aforementioned, cyber threats can lead to the following:

[1] Adel Abdul-Sadeq. The Danger of Cyber Wars in Cyberspace. Al-Ahram Magazine for Computers, Internet, and Communications, 2017, p. 32.

[2] Aziz Milhem Barbar. Network and Internet Security. Naif Arab University for Security Sciences, Cairo, 2008, p. 04.

[3] Muhammad Mukhtar. Can countries avoid the risks of cyberattacks?" Futuristic Concepts, Issue 6, Future Center.

[4] Muhammad Mukhtar, previous reference, p. 51.

[5] Muhammad Mukhtar, previous reference, p. 52.

- Destruction of websites on the information network.
- Email hacking.
- Breaching the confidentiality of correspondence.
- Defamation of individuals.
- Credit card theft.
- Software piracy.
- Destruction of software and information.
- Forgery of documents.[1]

THE THIRD TOPIC: CYBERSECURITY DIMENSIONS:

There are five dimensions of cybersecurity that we will discuss below:

FIRST REQUIREMENT: MILITARY DIMENSION

Cybersecurity demonstrates its strength in its ability to connect military units through military networks in cyberspace. This allows for easy information exchange, rapid issuance of military orders, and remote access to targets, and their destruction. However, this advantage can become a vulnerability if the network used is not securely protected from external breaches. This can lead to counter cyber-attacks on military networks, intelligence agencies, espionage on national security, disruption of rapid deployment of forces, or disruption of communication systems between military units and disabling computer networks. It can also result in the disabling of air defense systems, electronic guidance, and loss of control over command units.[2]

SECOND REQUIREMENT: ECONOMIC DIMENSION

Cyberspace has become attractive to all sectors of society. The reliance on digital technology for data and information storage, as well as the use of computers in industrial development and economic activities, has increased significantly. Financial and economic transactions are now computerized, and banking networks, stock exchanges, and financial markets are interconnected through electronic systems and networks. The Internet has become the foundation for financial and economic transactions and a major driver of economic development in the 21st century. This has led to discussions about the importance of achieving cybersecurity in the economic field.

THIRD REQUIREMENT: SOCIAL DIMENSION

Social media networks contribute to opening up opportunities for individuals to express their social aspirations and ambitions in various forms. The participation of different segments of society in using the internet allows for access to ideas and

[1] Amina Muhammad Al-Mukhtar, Amima Hamid Al-Ahmadi. Sharia Controls for Informatics. Informatics and Education, Dar Al-Zaman Library, Taibah University, Riyadh, 2005, p. 468.

[2] Hamdoun Touré. Cybersecurity in Developing Countries." International Telecommunication Union, Jordan, 2006, p. 15.

information. This necessitates the stability of cyberspace because the openness of society to other communities establishes the exchange of experiences, ideas, and the formation of cooperation and integration prospects.[1]

FOURTH REQUIREMENT: POLITICAL DIMENSION

Every state have the right to protect their political systems and economic interests to achieve the welfare of their people. Modern information means helping individuals access the backgrounds and justifications for political decisions made by their government through the vast amount of information they can access. Conversely, political actors utilize these technologies to reach the largest possible segment of individuals and promote their policies globally. This impact exists regardless of the validity of the policies, principles, and positions they promote[2]. Numerous examples highlight the importance of the political dimension of cybersecurity, such as leaks of sensitive documents causing problems in the relationships between countries, which necessitated a reconsideration of foreign policies in light of these leaks. Social media networks also play a prominent role in achieving political goals, such as organizing electoral campaigns, virtual demonstrations, and electronic protest movements. Additionally, some countries, like the United States, broadcast political messages on social media platforms to achieve their objectives, such as the U.S. military developing an electronic program to launch personal accounts on social media platforms in different languages, aiming to disseminate messages that support the American vision on social media. On the other hand, many terrorist movements have also found a presence on these platforms.[3]

FIFTH REQUIREMENT: LEGAL DIMENSION

The relationship between law and technology is reciprocal. Different technological developments necessitate the development of legal frameworks to regulate both legal and illegal activities. However, cybercrime currently lacks strict legal frameworks to deal with it. This is due to factors such as the nature of the electronic crime itself, the difficulty of identifying the perpetrators, the flexibility of definitions related to information technology, and the fact that cybercrime is not confined by national borders, which requires international cooperation to combat it.[4]

THE FOURTH TOPIC: CYBERSECURITY GOALS

[1] Nouran Shafik. The Impact of Electronic Threats on International Relations: A Study on the Dimensions of Cybersecurity." Arab Office for Knowledge, Cairo, 2014, p. 40.

[2] Adel Abdul-Sadeq, previous reference, p. 27.

[3] Abdul-Ilah Ahmed Halali. The Budapest Convention on Cybercrime." 1st Edition, Dar Al-Nahda Al-Arabiya, Cairo, 2008, p. 129.

[4] Abdul-Ilah Ahmed Halali, same previous reference, p. 135.

Cybersecurity aims to protect all operations we perform using the internet, technology, and various communication methods. It aims to protect data, and applications, and preserve national and individual information, preventing unauthorized access or tampering. A strong system is necessary to safeguard these services and the information provided by advanced technology through cyberspace.[1]

Multiple information risks should be considered when building and developing IT equipment and systems. These risks can compromise the confidentiality, integrity, or availability of information. They include the risk of denial of service, which prevents the use of IT resources and software, leading to system collapse and preventing their utilization. There is also the risk of infiltration and penetration, where unauthorized individuals gain access to information systems and resources, controlling or exploiting them to attack other resources and systems. Additionally, there is the risk of data theft, which can occur due to vulnerabilities in systems or equipment or the use of specialized software, allowing unauthorized individuals to access, steal, or manipulate stored or transmitted data.[2]

The term cybersecurity encompasses all aspects related to safeguarding services, data flow, and everything related to the use, mechanisms, applications, and technological equipment, as well as the interconnection through computer networks, communications, and the internet. Therefore, the goal of cybersecurity is to enhance the protection of electronic systems, information technology systems, operating technology systems, and all their components surrounding society, including devices, software, equipment, and everything that affects the progress of these services.[3]

Securing the infrastructure of information and citizens' data, and protecting the information network and communication is essential because the destruction, infiltration, or sabotage of this network would lead to communication disruption and the cessation of various electronic services, hindering various entities from performing their tasks. Cyberspace encompasses both physical and non-physical elements, including computer devices, networks, software, information processing, content, transmission and control data, and the users of these elements[4]. Protection aims to deter criminals from carrying out their plans or prevent them from

[1] Murad Mashoush. International Efforts to Combat Cybercrime." Hassan I University, Faculty of Legal, Economic, and Social Sciences, Business Law Research Laboratory, Morocco, 2018, p. 50.

[2] Same previous reference, p. 55.

[3] Muhammad bin Ahmed bin Ali Al-Maqssoudi. Cyber Crimes: Their Characteristics and Legal Confrontation. Arab Journal of Security Studies, Vol. 33, Issue 70, Naif Arab University for Security Sciences, Riyadh, 2017, p. 13.

[4] ITU , Cybersecurity, Géneva : internationaltélécummunication Union (ITU),2008. P 12.

achieving them and ensure an acceptable level of risk through a plan that aligns with the technical, human, organizational, and legal aspects.

THE FIFTH TOPIC: METHODS FOR ACHIEVING CYBERSECURITY

Preserving information and data is crucial for individuals, organizations, and even countries. While devices and software can be replaced, it is difficult to recover lost or manipulated data and information. Therefore, data and information are considered valuable assets for any organization, and efforts are made to protect them and restrict unauthorized access[1].

Several methods can be employed to achieve cybersecurity and counter electronic attacks, including technological, informational, educational, and security aspects, which are outlined below:

- Utilizing advanced protection techniques and software for email and official accounts that are antivirus capable and can counter electronic attacks. Enhancing security standards and systems and developing software resistant to cyber-attacks by equipping information security systems with the latest methods and technologies, especially artificial intelligence techniques.
- Relying on encryption to detect and trace potential attacks, establishing an early warning system to monitor anticipated cyber-attacks, and implementing effective encryption policies for sensitive data and information.
- Leveraging cloud computing systems to safeguard against data loss. By using cloud applications, data will not be lost in the event of device malfunction or shutdown.
- Engaging cybersecurity experts and specialists through various media platforms, providing continuous awareness to digital platform users about potential methods used by hackers to breach systems and sensitive data, and revealing their techniques, tricks, and technologies.
- Enacting comprehensive and precise legislation that addresses and keeps pace with the rapidly advancing technological threats and cyber risks.[2]
- Incorporating cybercrime combating systems into educational curricula at all levels to enhance digital security awareness. This would support the safe use of communication technology, develop students' research skills to build specialized professional frameworks in cybersecurity management and enhance their security awareness. This should align with the technological advancements in cloud computing and data management. International

[1] Amina Muhammad Al-Mukhtar, Amima Hamid Al-Ahmadi, previous reference, p. 478.

[2] Amira Muhammad Muhammad Sayed Ahmed. Strategies for Combating Cybercrimes in the Information Age." Journal of Media Research, Faculty of Media, Al-Azhar University, Issue 58, Part Four, Cairo, 2021, p. 179.

partnerships and agreements among universities should be established to increase the qualifications of professionals dealing with such electronic crimes.

- Imposing strict control on suspicious websites, preparing confrontation plans, implementing precautionary measures regularly, strengthening and updating operating systems, and improving the efficiency of programmers in designing programs and systems that are difficult to penetrate.[1]
- Conducting continuous training workshops on strategic cybersecurity intelligence and how to employ it in vital sectors to counter potential cyber threats.[2]
- Using passwords to access computers and changing them periodically, with the length of the period depending on the importance of the data. Additionally, some operating systems do not allow the reuse of the same password, forcing users to change it after a specified period set by the operating system administrator.
- Implementing internal control methods within the system that help prevent unauthorized access attempts. For example, creating a log file that records all individuals who have accessed or attempted to access any part of the data, including user ID, time and date of the attempt, the type of operation performed, and other relevant information.
- Encrypting important data transferred through communication channels, such as satellites or optical fibers, so that the data is encrypted and then returned to its original state upon reaching the receiving end. Data and information encryption should be utilized for important tasks, considering that the encryption process can be costly.
- Avoiding the disposal of information outputs, such as printer ribbons or information consumers, as such outputs may contain important information accessible to unauthorized individuals. Therefore, it is essential to shred the outputs, especially before disposal.
- Employing individuals whose task is to continuously monitor computer software to ensure its proper functioning, especially financial software that is often tampered with by programmers or users. This can be done by randomly sampling software outputs at different intervals and examining the monitoring file to identify individuals who have accessed or attempted to access the data.
- Creating backup copies of data stored outside the device location.[3]

[1] Same previous reference, p. 180.
[2] Same previous reference, p. 181.
[3] Amina Muhammad Al-Mukhtar, Amima Hamid Al-Ahmadi, previous reference, p. 480.

- The use of modern means to ensure that only authorized individuals have access to computer center departments, such as using devices that recognize eye, hand, …etc
- Cooperation between countries in the field of protecting and securing cyberspace, defense, and deterrence against terrorism, and confronting cyber security challenges[1]

THE SIXTH TOPIC: REGIONAL AND INTERNATIONAL AGREEMENTS FOR CYBERSECURITY

THE FIRST TOPIC: REGIONAL AGREEMENTS

Regional agreements align with the requirements to keep pace with the rapid evolution of cyber threats. Several initiatives have been established in this field, including:

- In 2002, the Commonwealth countries developed a model law to combat cybercrime, in addition to digital evidence legislation.
- In 2009, the Economic Community of West African States (ECOWAS) initiated a recommendation for combating cybercrime, forming the legal framework for member states' work.
- The Arab Convention on Combating Information Technology Crimes was introduced in 2011 to enhance cooperation among Arab countries in combating cybercrime and preserving their security and societal safety.
- The Budapest Convention on Cybercrime, adopted in 2001, is a groundbreaking step in international cooperation. It is the only agreement with extensive coverage and a large number of participating countries. It entered into force in 2004 and serves as a regional binding instrument for combating cybercrime by promoting harmonization between national laws and emphasizing the need to enhance investigation techniques, research, and cooperation among nations.[2]

THE SECOND TOPIC: INTERNATIONAL AGREEMENTS

At the international level, the United Nations has played a role in promoting cybersecurity, safety, and raising global awareness of cyber threats through its resolutions. Some significant resolutions include:

- A 1990 resolution on the law of cybercrime.
- A 1991 resolution on combating the criminal use of information and communication technologies.
- The establishment of the Group of Governmental Experts (GGE) in 2001, consisting of experts who began their work in 2004. They discuss existing

[1] Amira Muhammad Muhammad Sayed Ahmed, previous reference, p. 181.

[2] Mona Al-Ashqar Jubour. Cybersecurity: The Fear of the Era." Arab Center for Legal and Judicial Research, Beirut, 2017, p. 103.

risks in the field of information security and explore potential international foundations to strengthen the security of global communication and information systems.

- A special resolution in 2003 focused on cybersecurity and the ability to combat cybercrime.[1]
- A 2010 resolution on cybersecurity and an annex emphasizing the importance of states assessing the compatibility of their legislative frameworks and their capacity to combat cybercrime.

Despite the value of these efforts and resolutions at the international level, they remain insufficient and ineffective due to their lack of legal bindingness and enforceability.

Conclusion

Based on the key points discussed in this intervention, it can be concluded that achieving cybersecurity has become a priority for every country to secure its information networks and data from cyber threats. However, this can only be achieved through preventive measures, such as using advanced protection technologies and antivirus software for electronic devices and official accounts capable of countering cyber attacks. It also requires developing software that is resistant to cyber attacks by equipping information security systems with the latest methods and technologies. Additionally, creating codes to detect and track potential attacks and implementing comprehensive legislation that aligns with the rapidly advancing technological landscape are crucial steps to mitigate electronic threats and risks.

Furthermore, incorporating cybersecurity crime-fighting systems into educational curricula at all levels can promote a culture of digital security. This would support the safe use of communication technology and enhance students' research skills to cultivate a specialized professional workforce in cybersecurity management.

Recommendations

1. Enhance cooperation among countries in combating cyber threats and crimes.
2. Organize awareness campaigns through workshops, lectures, national and international events, and participate in television and radio programs to alert all segments of society to the dangers of cyber-attacks.

[1] Adel Abdul-Sadeq, previous reference, p. 334.

3. Collaborate with security authorities to monitor and track incidents of intrusion and cyber piracy reported by citizens.
4. Encrypt all electronic transactions to protect data and applications from hacking and electronic breaches.
5. Emphasize the use of cloud computing systems that safeguard against data loss in case of device failure or interruption.
6. Provide continuous training for information security specialists, enhancing their knowledge and skills to ensure constant protection of information networks and stay updated with the latest technologies related to countering cyber-attacks.

Bibliography list:

1. Abdel-Fattah Bayoumi. Principles of Criminal Procedures in Computer and Internet Crimes. Dar Al-Kitab Al-Qanuniya, Egypt, 2007.
2. Abdulilah Ahmed Hilali. Budapest Convention on Cybercrime. 1st edition, Dar Al-Nahda Al-Arabiya, Cairo, 2008.
3. Adel Abdel-Sadek. Electronic Terrorism and Power in International Relations: New Patterns and Different Challenges. Center for Political and Strategic Studies, Cairo, 2009.
4. Adel Abdel-Sadek. The Threat of Cyber Wars in Cyberspace. Al-Ahram Magazine for Computers, Internet, and Communications, Cairo, 2017.
5. Amira Mohamed Saeed Ahmed. Strategies for Combating Cyber Crimes in the Information Age. Journal of Media Research, Faculty of Media, Al-Azhar University, Issue 58, Part Four, Cairo, 2021.
6. Amjad Al-Munif. Electronic Terrorism - A Modern Battle. Al-Arabia Magazine, Issue 7, Riyadh, July 2015.
7. Amna Mohamed Al-Mukhtar, Omeima Hamid Al-Ahmedi. The Legal Controls of Informatics. Informatics and Education, Dar Al-Zaman Library, Taibah University, Riyadh, 2005.
8. Aws Majid Ghaleb Al-Awadi. Cybersecurity: Cyber Information Security. Bayan Center for Studies and Planning, Beirut, 2016.
9. Aziz Malham Barbar. Network and Internet Security. Naif Arab University for Security Sciences, Riyadh, 2008.
10. Hamdoun Toure. Cybersecurity in Developing Countries. International Telecommunication Union, 2006.
11. Hassan bin Ahmed Al-Shahri. Advanced Digital Electronic Systems for Information Confidentiality and Protection against Espionage. Al-Noor Center for Electronic Research, Cairo, 2010.

12. Idris bin Tayeb Atiya. The Phenomenon of Terrorism in the Post-Modern Era: An Analytical Study of Forms, Methods, and Countermeasures. Arab Journal of Security Studies and Training, Volume 31, Issue 63, Riyadh, 2015.
13. ITU, Cybersecurity, Geneva : international telecommunication Union (ITU),2008.
14. Joseph. s Nye: JR; Cyber-power, Harvard Kennedy School,2010.
15. Mohamed Mukhtar. Can States Avoid the Risks of Cyber Attacks? Concepts of the Future, Future Center for Research and Development, Cairo, 2015.
16. Mona Al-Ashqar Jubour. Cybersecurity: Challenges and Requirements for Confrontation. Arab Center for Legal and Judicial Research, Cairo, 2012.
17. Mona Al-Ashqar Jubour. Cyberspace: The Concern of the Era. Arab Center for Legal and Judicial Research, Beirut, 2017.
18. Muhammad Al-Amin Al-Bashiri. Investigation of Computer Crimes. Research paper presented at the Law, Computer, and Internet Conference held at the Faculty of Sharia and Law in the United Arab Emirates, 2000.
19. Muhammad bin Ahmed bin Ali Al-Muqsoudi. Cyber Crimes: Characteristics and Legal Confrontation. Arab Journal of Security Studies, Volume 33, Issue 70, Naif Arab University for Security Sciences, Riyadh, 2017.
20. Murad Mashush. International Efforts to Combat Cybercrime. Hassan I University, Faculty of Legal, Economic and Social Sciences, Business Law Research Laboratory, Morocco, 2018.
21. Noran Shafik. The Impact of Cyber Threats on International Relations: A Study on the Dimensions of Cyber Security. Arab Office for Knowledge, Cairo, 2014.
22. The international telecommunication Union, (ITU) Toolkit for cybercrime legislation, Geneva, 2010.