

The Dangers and Threats of Cyberspace for National Security: The Case Study of Egypt and Cyberterrorism

Magdy M. Eldagher ⁽¹⁾

¹⁻ Mansoura University – (Egypt), E-Mail : eldagher@mans.edu.eg

Received: 20/02/2025;

Revised: 01/04/2025;

Accepted: 08/05/2025;

Abstract:

Egypt is one of the countries that suffer from major security breaches by groups and organizations of violence and traditional and electronic terrorism. Therefore, this part will address the issue of the threats posed by the digital space to Egyptian national security, by focusing on the phenomenon of electronic terrorism and the efforts made by the Egyptian government and the security establishment to confront this phenomenon. And its regional and international impacts, The results indicated an increase in the rates of electronic crimes, which varied between promoting rumors, spreading vice, and terrorist violence, in addition to bullying, fraud, and electronic blackmail, and the growing role of actors, including activists, committees, electronic armies, and non-state actors in the cyber field, Study Proposals : Increasing awareness of the danger of cyberterrorism and ways to combat it using the latest technological technologies, while raising the necessary capabilities to develop and implement Egyptian strategies related to combating cyberterrorism.

Keywords: Cyberspace, National security, Cyber threats, Cyber terrorism, The Dangers.

Introduction:

There has been an interest in cyberspace recently, and this has been evident in many states governments' adoption of multiple security policies and developing programs based on securing information systems that have become a threat to the security of countries, which has prompted many researchers to say that cyberspace is the strongest threat to national security in the twenty-first century. [1]

As a result of the above, many countries in the world have adopted a number of initiatives to protect the information infrastructure from the risk of exposure to cyber threats and have worked to find new legislative frameworks and adopted legal procedures that would address non-traditional threats such as terrorism and electronic espionage. [2]

In addition, many developed countries sought to adopt international initiatives to secure their cyberspace, the most important of which was the International Partnership to Combat Cyber Terrorism (IMPACT) initiative, which aims to mobilize international efforts and civil society to confront the growing threats posed by

* Magdy M. Eldagher

cyberterrorism. The initiative also sought to collect visions and ideas. About the exchange of experiences in combat methods between countries of the world [3] which was a meeting point that brought together information security experts and security institutions in order to discuss the danger of electronic terrorism and how to confront it, such as the “SITE” group “which is based on monitoring terrorist ideology via the Internet and monitoring advocates of violence on social media networks and elsewhere.” [4]

In this context, many European governments began to develop national frameworks and strategies and understand the extent of their dependence on the Internet and the vulnerabilities of protection programs in order to secure the networks and infrastructure on which their digital future depends, while a number of Arab governments decided to intervene in cyberspace and oblige institutions and sectors to disclose the shortcomings in its protection programs, in addition to obligate individuals themselves to send notifications and report any breach that occurs on their phones and mention the type of data that was exposed to risk and the technology used in that. [5]

Given the importance of cyberspace, terrorist organizations have exploited the advantages of modern technology to support and achieve their goals and support their criminal activity around the world. Terrorist organizations have been able to carry out many of their operations with ease, relying thus on advanced technologies such as “cloud computing and encryption software, and penetrating and harnessing network systems.” in criminal operations that have been remotely targeted the security of countries. [6]

In summary, the study aims to identify the risks and threats that cyberspace poses to Egyptian national security by applying it to the phenomenon of cyberterrorism in the light of the available strategies.

Study Problem:

As a result of technological development at the international level, it was natural for most countries in the world to adopt many digital technologies that are internationally popular. This transformation had negative effects and threatened the security of countries through hacking the websites of governments and their institutions and spying on them, leaking and publishing military secrets, and penetrating banks and stock exchanges, which negatively affects the economic security of countries and international security as well.

In this context, Egypt was not far from the negative effects of cyberspace after the January 2011 revolution, as it was also exposed to political and economic threats and operations aimed at spreading religious extremism among young people trying to lure them with money and religious slogans towards acts of violence and terrorism. As a result of these threats, Egypt utilized a number of means and effective tools to confront the phenomenon of terrorism coming from the Internet and strive to develop a national strategy that contributes to real stability of the state from any potential threat.

On its part, the “Cybersecurity Index” issued by the International Telecommunication Union reveals that Egypt during 2022 ranked 23rd globally among 182 countries in the volume of cyber breaches, while America topped the index with a score of 100, and the Egyptian government was quick to take steps towards protecting its national security through establishing a higher council for cybersecurity and developing a national strategy for cybersecurity, in addition to launching the National Center for Computer Emergency Preparedness (EG-CERT). However, despite all these measures, the effects of cyberspace on Egyptian national security are still present and in high rates as a result of suppression of freedoms and economic crises facing the Egyptian government and the large number of rumors surrounding them . [7]

Hence, the problem of the study is crystallized in identifying the risks and threats that cyberspace poses to national security by applying it to the phenomenon of electronic terrorism in the light of the national means, tools and strategies used.

Importance of the Study:

The importance of the study comes from the fact that it sheds light on modern communication technologies that have a significant impact on the national security of countries. The importance of the study also highlights the position that cyberspace has occupied, which has become a highly targeted field that threatens the national security of countries, in addition to being an attempt to enrich the Arab library with the study of a new study that deals with electronic terrorism and national security issues.

It is expected that the intended results will be used to identify the extent of the impact of cyberspace on Egyptian national security. These are indicators that may become useful to decision-makers and workers in security institutions and others.

Objectives of the Study:

The study aims to highlight the Egyptian role towards renewing the security system in the light of modern requirements, and developing classic methods in security work through openness to the virtual field and employing new methods and tools through which the Egyptian government can protect national security and protect society from the dangers of electronic terrorism. It also aims to knowing the extent of the impact of cyberspace on Egyptian national security issues, and the Egyptian government’s efforts to confront modern electronic risks, which undoubtedly lead to the state protecting its infrastructure with more effective national methods and strategies.

Study Questions:

The study is based on one main question: “What is the extent of the impact of cyberspace on Egyptian national security issues in application to electronic terrorism?” From the main question come the following sub-questions:

- What is the extent of the impact of cyberspace on Egyptian national security issues?
- What are the most prominent risks and threats of cyberspace to Egyptian national security?
- What are the means that pose a danger and threat to Egyptian national security?

-
- What are the tools used by terrorist organizations to harm Egyptian national security?
 - What is the nature of the Egyptian national strategy to deter and protect Egyptian national security?

Study Hypotheses:

The study presents two hypotheses within the framework of realist theory, The first indicates that “the more the state succeeds in increasing the level of cyberspace, the more this will contribute to protecting its national security.” The second hypothesis indicates that “the more cyber risks and threats against the state increase, the more its level of national security will decrease.”

Study Concepts and Terminology:

- National Security: is providing protection for citizens and individuals present on the territory of the state, away from the occurrence of crises that lead to human, financial and technical damages. [8]
- Cyber Terrorism: It is an organized attack by terrorist groups on the infrastructure, systems and networks of countries with the aim of sabotaging and threatening their national security. [9]
- Cybersecurity: means protecting existing systems, data, communications, and networks connected to the Internet from cyberattacks, such as attempted hacking or illegal entry all the way to destroy the infrastructure of major countries' institutions or bodies and institutions. [10]

Previous Studies and Researches:

By reviewing the scientific literature in the database of universities and research centers, the researcher was able to access a limited number of studies that intersect with the current study in some of its aspects. Among these studies is ,Sharifa Kalaa (2022) [11] was concerned with cybersecurity by focusing on the challenges and risks that threaten the security of countries, and ultimately achieves what is known as national cybersecurity. The study reached the fact that whoever owns advanced technology will certainly have great influence in cyberspace and achieve cybersecurity through which supports the national sovereignty of his country, while the study of Hatem bin Azzouz (2022) [12] dealt with the dialectical relationship between cybersecurity and cybercrime in the United States of America, and indicated The study pointed to the high use of the Internet in vital institutions in the United States, and the results found that the repeated exposure of US financial and military institutions to hacking and data theft, prompted the government to make cybersecurity a priority in all its vital institutions.

On the importance of national security and cybersecurity challenges, the study of Masbaka Mohamed (2022) [13] focused on cyberspace and national security challenges in the Arab Maghreb countries, and the study raised many questions, the most important of which is "To what extent can cyberspace pose a threat to the national security of the state? The answer came through three axes: the concept of

national security and its dimensions, cyber threats to national security, cybersecurity as a guarantee of national security, and the results concluded that the countries of the Arab Maghreb and North Africa do not have adequate means of protection from cyberspace threats.

Youssef Jamal's study (2022),[14] was more focused on the threats of social networking sites and the importance of activating security media in Algeria, as the study revealed the interest of the General Directorate of National Security in Algeria to follow up on the threats published on Facebook to individuals and topics that affect state security, and the results of the study reached the importance of social networking sites in exchanging content between users, and recommended the need to create special electronic accounts for national security in Algeria that can be referred to in times of crises and important security events , This is confirmed by the study of Talla and Lamia (2020) [15], where cyberspace has become part of modern methods of warfare and a tool that is used in the attack on the security of states, and the study demanded that cybersecurity become a strategic weapon in the hands of governments to ensure the preservation of the security and stability of countries, and the study of Hazem Musa (2020) [16] came to put forward a strategic vision to protect Iraqi national security, as the study focused on the possibility of building a strategic vision for Iraqi national security in light of threats The study called for the need to work to protect cyberspace by establishing a Ministry of Cybersecurity in Iraq.

On the other hand, the study of Fatima Zahra Ashour (2018) [17] was concerned with monitoring the impact of cyberspace on national security in Algeria, and the negative use of Internet sites, which was the cause of many security threats and which has become more vulnerable due to the ease of penetrating information through communication networks that are linked to unknown parties, and the study called for the need to take many ways to protect cyberspace in Algeria, which was confirmed by the study of Ihab Khalifa (2014) [18], and space capacity. The results concluded that cyberspace is no longer the monopoly of the state, and that the expansion of the ease of ownership would push terrorist organizations to use it against the security and stability of countries, as the study of Richard Clarke, (2012) [19] confirmed that cyberwarfare is not a clean war and that it targets the security of states, and the study of Adel Abdel sadiq (2006) [20] which concluded that the use of cyberspace has become available to actors from non-states, which may affect the sovereignty of states.

From the above, through previous studies, the researcher was able to confirm the soundness and validity of the idea of his study and enrich its axes at the cognitive, theoretical and applied levels. Benefiting from them lies in comparing the results and recommendations reached by these studies with the results of the current study.

Agree and disagree with the current study:

From the presentation of previous studies, the researcher notes that the subject of cyberspace is a new topic, which still enjoys the attention of researchers in political and social sciences in Arab and international universities, and that the majority of previous studies agreed on the danger of cyberspace on the national security of countries, and that this threat has political dimensions that may lead in some stages to

the declaration of war with tools that did not exist in previous wars, but what distinguishes the current study comes through the specificity of the state (Egypt) as one of the most countries in the world. Affected by terrorism and piracy, in addition to that Egypt is one of the countries that suffer from many security breaches by political Islam groups, which affects the security and stability of the state at home and its external reputation, so the study will address the threats posed by cyberspace to Egyptian national security, focusing on the phenomenon of electronic terrorism and the efforts made by the Egyptian government and security strategies to address this phenomenon and its regional and international effects.

Theory Explaining the Study: (Realistic Theory)

Realist theory has dominated studies of security and international relations for many years, as this theory seeks to explain the mechanism of the process of the international system and the reason for the occurrence of conflict and strife between countries in cyberspace, according to the writings of Edward Carr and Hans Morgenthau. [21] Realist theory assumes that war and conflict are two phenomena that are likely to occur due to the chaos of the international system and the lack of a supreme authority above states. In the light of this chaos, states are interested in searching for national security based on their own capabilities and increasing their military and economic capabilities through alliance with other countries.

The realist theory relies on two main axes:[22]

- The axis of power: It is a major determinant of international behavior, as in the absence of institutions and procedures to resolve conflicts in international relations, states remain strong, and the pursuit of power is the cause of international conflict.
- National interest: In which achieving the national interest of the state is the main goal of its foreign policy, and therefore national policy is the main driving force of the foreign policy of any country, and therefore the national security of countries is mainly related to how far these countries are able to get into war to ensure the protection of their national interests.

Type and Method of the Study:

The study belongs to all descriptive studies, and uses the descriptive analytical method, which means carefully collected the available documents about the research problem and then analyzing them in a way whereby the researcher can conclude what is related to the problem of his study. The study also relied on qualitative analysis by extracting evidences and proofs from the sources, references and documents that dealt with the relationship between cyberspace, national security, and electronic terrorism.

- Data Collection Tools: The study relied on the content analysis tool of scientific literature, including studies, researches, reports, and published materials on the subject of the study, as it is one of the research methods used to describe apparent or explicit content in an objective, systematic and quantitative manner.

First : The Dimensions and Impact of Cyberspace on the Security of States . [23]

Cyberspace has become a new arena for competition between international actors and non-state actors. Hence, cybersecurity has played an important role in giving some characteristics to international conflicts between actors, including: cyber power, which has become an arena for great powers and an alternative to traditional power in the light of the increasing militarization of cyberspace. In addition to the cyber arms race between the active powers in the international system in the light of a global system that combines conflict and cyber protection as an entry point to rebalancing powers in the new world order.

Although the prevailing reactions to cyber threats call for the inevitability of cooperation, and the importance of disclosure and serious participation in confronting them, political variables may stand in the way of achieving this, which confirms the importance of civil society in urging governments to overcome the conflict and move towards protecting international security. In the light of this, researchers in many universities and research centers were busy developing old traditional concepts such as soft power and cyberspace, most notably the Belfer Center for Science and International Affairs, [24]

Kennedy University and Harvard, where the results of their findings confirmed that power is what the state possesses in terms of electronic targets for one or more patents. The inventions announced annually, and the number of global security companies, leading to calculating expertise and technical capabilities by measuring the number of government initiatives as determinants of the state's power in cyberspace, which can be summarized in the following points: [25]

In 2017, governments, companies, and individuals were subjected to global piracy, as a ransom program called WannaCry targeted some vulnerabilities in Microsoft Windows operating systems and infected millions of computers in 150 countries in various business sectors. In Britain, the same program, WannaCry, infected at least 81 entities working in providing 236 national health services, which affected the health and safety of patients. [26]

In June 2017, another ransom program called NotPetya was launched targeting global commercial companies connected to the Internet using the "doc.me" accounting program update mechanism. Within minutes of its launch, it infected thousands of systems in more than 65 countries, including government institutions, banks, and companies. The NotPetya program also targeted a company, A.P. Moller-Maersk, which is the largest shipping company in the world, and the virus wiped out the information systems of the company and its branches in countries around the world. As a result, Maersk was forced to stop its operations in 76 ports around the world, as estimates of Maersk's losses due to NotPetya amounted to about \$300 million, and the company was forced to rebuild its infrastructure with (4,000 new servers, 45,000 new computers, and 2,500 new applications), and in total the losses caused by NotPetya were estimated at \$12 billion due to the disruption of maritime traffic in the world alone. [27]

Saudi Aramco was also not spared from acts of piracy, as it also fell victim to the Trisis virus - in August 2017 AD, which is a virus that aims to sabotage industrial control systems (ICS) in oil and gas facilities and safety security systems. The attacks on the company continued until 2021 AD ,[28]

table No. (1) explains

Ranking of the world's countries according to the Global
Cyber power Index,

2023 index	2022 index	2020 index	2018 index	2011 index
America	America	America	Britain	Britain
Britain	China	China	America	America
Estonia	Russia	Britain	France	Australia
korea c	Britain	Russia	Lithuania	Germany
Russia	Australia	Holland	Estonia	Canada
Lithuania	Holland	France	Singapore	France
Japan	korea c	Germany	Spain	korea c
Canada	Vietnam	Canada	Malaysia	Japan
France	France	Japan	Canada	Italy
India	Iran	Australia	Norway	Brazil

Statistical data from the (Belfer Center for Science and International Affairs, Harvard University, Al Jazeera Center for Studies, Al Arabiya Net website,2024)



- Based on the indicators of the previous table, the researcher notes that despite the many positives that have been achieved through the use of information and communications technology in various vital sectors of countries, it has been accompanied by a number of negative effects as a result of misuse, most notably cybercrimes, which has created a new type of crimes that cross borders and continents, and whose effects are no longer limited to a specific country, and therefore it was natural for the negative effects to take three forms, which are as follows .[29]

- Cybercrimes include (hacking, spreading viruses, cracking codes, network intrusions, cyberstalking, data tampering, identity theft, credit card fraud, software piracy...)
- Electronic attacks include (malware, phishing, social engineering,)
- Cyber terrorism includes (manipulating and disrupting information systems and destroying virtual and physical assets by using computer viruses, worms, Trojan horses, ransomware attacks, and hacking designed to demolish and sabotage websites....)

Second,: The Importance of Cyberspace in Countries' Priorities:

The danger of cyber threats lies in the fact that they are capable of inflicting great losses on the party that is exposed to them, because these threats may take many levels and forms, including: cutting off communication systems between military units, manipulating the state's economic and financial data, or erasing them from computers, or controlling Artificial Intelligence systems and directing them to carry out acts of sabotage, which may be due to the following. [30]

Governments' interest in cyberspace has increased, which has expanded the possibility of infrastructure being threatened, The decline of the role of the state in the light of globalization and its withdrawal from some strategic sectors in favor of the private sector, The emergence of a new pattern of damage due to cyber-attacks, with no need for any physical entry into its territory, Transforming cyber wars into one of the tools for influencing information in the various stages of conflict, Utilizing cyberspace to maximize the power of countries by creating an advantage or influence in different environments, The widening scope of risks of hostile activities practiced by actors, whether state or non-state.

The Impact of Cyberspace Actors on the Security of Countries:

Joseph Nye considers electronic power to be a concept that indicates the ability of virtual networks to play an influential role in the management of international units. Nye identified three types of actors who possess power and influence: .[31]

-The State: The State is considered a major actor in the management of cyberspace, based on its material, human, legal and structural capabilities. It possesses the ability to carry out electronic attacks, develop infrastructure and exercise authority within its borders. [32]

-Non-State Actors: This is where groups, non-governmental organizations, and multinational companies come into play. This category is capable of making intrusions into websites and carrying out terrorist acts. They do not have the capabilities of the state itself in terms of virtual attacks, but they pose a threat to the international environment, including "multinational companies, organizations." Criminal, terrorist organizations. [33]

-Individuals: Individuals possess technological knowledge and the ability to employ it, despite the difficulty of pursuing transgressors and revealing their identity, and they are often called hackers or hackers. [34]

Third: The Problem of the Phenomenon of Terrorism in Cyberspace:

The concept of "cyber-terrorism" refers to committing terrorist acts by using information technology and communications technology systems. Some define it as a new technological tool for traditional terrorism that transcends national borders and is capable of influencing the interests of states and their institutions. It aims to incite panic and fear among the civilian population and push governments towards imposing policies and making decisions that may not be consistent with their stated political vision.

Cyber terrorism is the point at which terrorist action intersects with cyberspace, and in this sense, it differs from cyber-crimes such as: data theft and bank fraud, where cyber terrorism targets people, property, or the infrastructure of countries, causing significant damages that may reach the point of injury, death, major economic losses, etc. [35]

The phenomenon of electronic terrorism may take one of two forms: either attacking data, as stealing and destroying data may lead to the failure to provide cyber services. As for attacks that focus on control systems, they aim to disrupt infrastructure such as the energy supply network, railways, water supplies, and electricity power stations by using a special electronic bomb called CBU 49, from which several bombs are released in the air targeting power stations and leading to their burning and destruction in addition to the complete disruption of communication services in times of crises.

In the same context, terrorist organizations have expanded their use of cyberspace applications for "propaganda, recruitment, spreading extremist ideology, collecting money, stealing data, conducting communications, training, and planning new terrorist operations. [36]

ISIS was able to hack the Malaysian Airlines website and control the radio broadcasting sites, the French television channel TV5 and its affiliated stations, and their accounts on Twitter, Facebook and Instagram. They were also able to hack the accounts of the US Military Central Command on YouTube and Twitter. The Military Central Command logo was replaced with an image of a bearded man with the words "Cyber Caliphate" and "I Love You ISIS" underneath on Twitter, in addition to the organization publishing two pro-ISIS video clips on their YouTube account, as well as publishing personal information for some US army commanders, including their names, phone numbers, place of residence, and their children's schools. [37]

Terrorist organizations also exploited cyberspace to launch the Caliphate Cyber Army, whose mission is to attack British websites, especially the Ministry of Health website. The website pages were replaced with pictures of the Syrian war, graphic drawings bearing the words "Stop the killing in Syria," and hashtags bearing phrases such as: #Op-Russia and #Save-Aleppo, and its channels on "Telegram" were hacked and videos were released under the title "Raqqa is Being Slaughtered Silently," along with news of crimes committed against civilians in Syria. [38]

Accordingly, terrorist organizations may use Internet applications to spread and manage terrorist propaganda. Especially since this propaganda is difficult to broadcast through traditional media, ISIS had seven media agencies, the most prominent of which is Amaq, which includes 37 media offices in different countries.

In contrast, Al-Qaeda has a media arm called Sahab. It is based on spreading jihadist ideology on the Internet, and within this framework two types of terrorism have emerged: They are pure cyber terrorism and hybrid cyber terrorism. [39]

both of which represent a threat to the national security of countries, as cyber terrorism in this sense includes hacking websites, piracy, spreading terror, and attracting individuals towards acts of violence, terrorism, and others. Hence, these negative uses of cyberspace show the danger and threat that electronic terrorism represents to the national security of countries on the part of actors in the information society, especially terrorist organizations and organized gangs, which represents a threat to national and international security in general.

Methods used by terrorist organizations to threaten the security of countries:[40]

The risks and threats to the national security of countries vary as a result of the negative use of cyberspace applications by terrorist groups and organizations, which can be summarized as follows: [41]

- Electronic Piracy: This is done by modifying, sabotaging, or deleting content, known as website piracy, and disrupting computers and networks that provide the service.

- Electronic Espionage: It usually targets institutions, government agencies, and large companies.

- Electronic Terrorism: It usually comes through organizations that adopt violence and practice terrorism against devices, networks, and information, which leads to material damage and damage to public and private property.

- Electronic Warfare: It aims to influence the political will of decision-makers in the electronic field or at the level of military or civilian action. [42]

Fourth,: Threats of Terrorist Organizations to Egyptian National Security:

There are many threats to Egypt after the January 2011 revolution. The results of a study by Kaspersky, a company specialized in cybersecurity, showed that Egypt was subjected to about 13 million cyberattacks during the first quarter of 2023, including bank accounts and customer data by 186% . [43]

This indicates a significant increase in piracy rate targeting the banking sector in Egypt, in addition to an increase in phishing attacks via email and SMS. According to a recently published study, 115,000 users in Egypt in 2023 were exposed to phishing attacks, in addition to a number of government institutions were attacked by international hackers with the aim of espionage and stirring public opinion against the ruling regime in 2023. [44]

In the face of these facts, the confrontation of the government and its security institutions was weak in the light of the Muslim Brotherhood's employment of what is known as "electronic committees," which tried through its channels to spread chaos in society, undermine stability, spread rumors due to the economic decline, and cast doubt on the state's national projects. In the same context, the use of "Twitter" by the "Bayt al-Maqdis Group" is notable, which is the group that changed its name years ago to "Wilayat Sinai" after announcing its allegiance to ISIS. The "Soldiers of Egypt Group" also launched pages on the "Twitter" and Facebook" websites to incite against the army and police and explain the manufacture of hand grenades and how to use them against security institutions in Sinai. [45]

As for the Muslim Brotherhood, it was keen on using Internet applications to spread its ideas. It launched a number of its affiliated websites, such as: "Ikhwan Online" in 2003, "Ikhwan Web" in 2005, "Ikhwan Wiki" in 2009, "Ikhwan Book" in 2010, and the "Rasd" network in 2011. The group was also more active through personal blogs and social networking sites such as Twitter, Facebook, YouTube, and Instagram, which are platforms that have become major tools for mobilizing and calling for demonstrations against state institutions. [46]

The Brotherhood was also active on the "Telegram" application in 2019, and reliance on it was 20%, while "Twitter" was 28%, "Facebook" was 22%, "YouTube" was 18%, and smartphone applications were 12%. Believing in the secret work followed by the group, the "Brotherhood Committees" turned to the "Clubhouse" application, which facilitated the recruitment process and inciting the elites against the ruling regime in Egypt. [47]

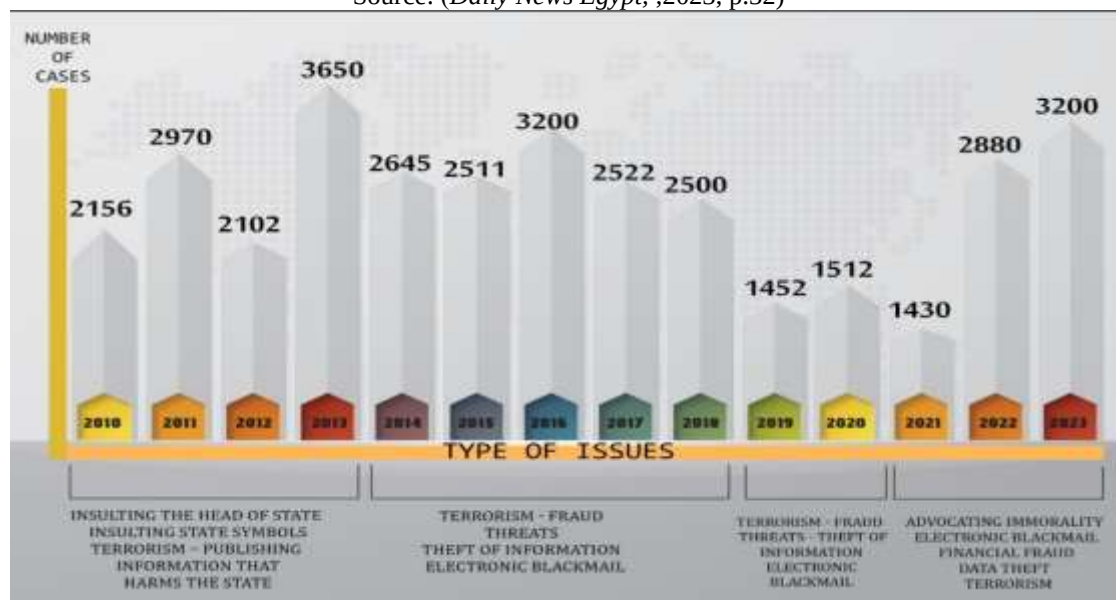
As for Al-Qaeda and ISIS, each of them sought to build cyber capabilities that would allow them to carry out attacks against state institutions remotely, which means that ISIS was able to achieve many of its goals through Internet applications, in addition to artificial intelligence techniques. Encryption, fifth generation networks, and Blockchain, and using them to collect information about security institutions and the families of their workers and incite against them.

.Table No. (2) the number of associated cases
Cybercrimes in Egypt during the period (2011-2023) [48]

Type of issues	Number of cases	the year
Insulting the head of state - insulting state symbols - terrorism - publishing information that harms the state	2156	2010
	2970	2011
	2102	2012
	3560	2013
Terrorism - fraud - threats - theft of information - electronic blackmail	2645	2014
	2511	2015

	3200	2016
	2522	2017
	2500	2018
Violation of privacy - hacking - credit card theft - espionage - terrorism	1452	2019
	1512	2020
Advocating immorality - electronic blackmail - financial fraud - data theft - terrorism	1430	2021
	2880	2022
	3200	2023

Source: (Daily News Egypt, ,2023, p.32)



Fifth, International and Regional Efforts to Secure Cyberspace:

The international discussion on cyber risk management emerged at the World Summit on the Information Society (WSIS), a global gathering of the ICT community, where 170 countries decided to take advantage of the opportunities that information technologies can provide by improving access to infrastructure and technology information; development of communications technology; encouraging international cooperation to manage risks and threats to countries' national security. [49]

The Organization of American States (OAS) was the first to pay attention to information security in 2004, as the organization sought to build cybersecurity capabilities in member states through training and virtual crisis management.

In 2007, the International Telecommunication Union (ITU), an international agency of the United Nations specialized in information and communications

technology, announced standards for cybersecurity (GCA), which are “legal measures; technical measures, organizational structures, capacity building, and international cooperation.” These standards were this lead to the emergence of the National Cybersecurity Guide of the Union (ITU), which was followed by many agreements and initiatives, most notably the following: [50]

Cyber Arms Control Agreement: Many countries in the world have tended to enhance their cyber capabilities, in addition to protecting their national information infrastructure, by striving to possess technology and protection systems of all kinds.

Tallinn Law: It is subject to the European Union, where a legal instrument called the “Tallinn Guide” was announced in 2013, prepared by a group of international law experts with the support of NATO. [51]

International Agreements: The 2001 Budapest Agreement was a pioneering step at the level of international cooperation. Although the agreement provides some legal solutions for crimes such as piracy, it does not address the most threatening cyber-attack operations such as espionage to obtain data and information illegally.

International Telecommunication Union: The Union has established a specialized team concerned with smart networks and collecting and documenting information in order to prepare recommendations to support the communications system and increase its effectiveness in addressing cyber risks .[52]

In the same context, efforts made to secure cyberspace vary through the following: [53]

Building Cyber Armies: Most countries in the world seek to form cyber armies “electronic committees” and have allocated huge budgets for this to develop the attack and defense system and protect the infrastructure environment.

Launching a National Cybersecurity Body: A large number of countries around the world are seeking to form specialized bodies in cybersecurity whose mission will be to prepare the national strategy for cybersecurity, and develop policies, governance mechanisms, and guidelines related to cybersecurity, risk management, encryption standards, and others.

National Legislation for Cybersecurity: Many countries of the world have launched legislation and laws to confront cyber threats, and deterrent penalties have taken a large part of these laws, in addition to that most European and Arab countries have added to their constitutions legal texts and materials related to cybercrimes.

Sixth,: Procedures Regulating Cyberspace in Egypt:

National security issues in Egypt have important organizational, legal and technical dimensions, which are as follows:

Regulatory Framework: The Ministry of Communications is the body concerned with protecting cybersecurity in Egypt, and within this framework it worked to formulate effective protection strategies and plans, such as the National Telecommunications Plan 2000, and the National Strategy for Information and Communications Technology 2007, and in 2013 the Ministry announced the “2020 Strategy” which focused on 3 main goals: transforming towards a digital society, developing the

information and communications technology industry, and transforming Egypt into a global digital center. [54]

Legal Framework: Egypt has signed a large number of international agreements related to cybersecurity, including the Intellectual Property Law of 2002, the Communications Law of 2003, and the Electronic Signature Law of 2004, in addition to the Children's Law of 2008, the Economic Courts Law of 2008, as well as articles The Penal Code of 1937, the Criminal Procedure Code of 1950, and the Civil Status Law of 1994; Article 72 of the Civil Status Law criminalizes viewing or obtaining information stored on computers or disposing of it. [55]

Technical Framework: A number of bodies have been established to contribute to achieving Egyptian national security, the most important of which are:

The Egyptian Center for Information Emergency Response (CERT): The center was established in 2009 through the National Telecommunications Regulatory Authority. The center seeks to follow up and analyze various cyber risks, and coordinate with various parties to confront threats to networks and their service centers. The center considers that electronic viruses, external attacks and attempts of obstruction and penetration are threats to Egyptian national security.

Information Technology Industry Development Authority: This authority was established pursuant to Law No. 15 of 2004, and its basic competencies include supervising the implementation of the Electronic Signature Law. [56]

The Supreme Council for Cybersecurity: A higher council concerned with infrastructure and information security was established in 2014, called the "Supreme Council for Cybersecurity." The council's primary role is "developing a strategy to confront cyber risks and supervising its implementation." The decision to establish the council raised concern. A number of Internet activists have expressed concerns about the council's goal; Is it really against the electronic threat, or is it interested in monitoring citizens as well?

Laws Regulating Cybersecurity in Egypt: [57]

Law on Combating Electronic and Information Crimes No. 175 of 2018 AD. This law is considered the basis of cybercrime legislation in Egypt, as the law regulates the penalties imposed on illegal access, violations of individuals' privacy, and other forms of electronic violations.

Law No. 151 of 2020, regarding the protection of personal data: This law aims to protect individuals' personal information and set a new standard for data protection, which affects cybersecurity in Egypt.

Communications Regulatory Law No. 10 of 2003, which regulates legislation related to digital communications, and includes important guidelines to ensure the safe handling of personal data and protect Egyptian national security.

Sources of the National Security Threat in Egypt:

Despite the positives of virtual space, it entails a number of risks. It has become an arena for a number of actors who commit crimes punishable by law, such as insult,

slander, and defamation, as cyberspace in Egypt is exposed to a number of threats, most notably the following: [58]

Extremist Groups: Extremist groups - thanks to the digital means they possess - resort to a number of advanced technologies to recruit social media users into acts of violence against the state.

Incitement and Spreading Rumors: Since 2011, Egypt has faced a large number of rumors of all kinds, and social media networks have contributed to spreading and promoting many of them. Examples of rumors that spread after June 30, 2013, include the rumor of divisions and splits in the army and police and the people's agitation against them.

Increasing Crime Rates: Cybercrime rates increased in Egypt following the January 2011 revolution, while their goals varied from revenge to blackmail, theft of personal accounts, fraud, and impersonation. [59]

Egyptian Efforts to Secure Cyberspace:

The Egyptian government paid great attention to cyber threats, and quickly took many measures and procedures to regulate cyberspace, protect data at all levels, and address the challenges resulting from the cyber threat on its soil. For its part, the security institution (National Security, General and Military Intelligence) has placed cybersecurity among its priorities, similar to the countries of the world, as it hastened to review its security policies and include new methods concerned with information security while developing the infrastructure related to information technology in its institutions. This came as a result of Egypt being exposed to many threats and the emergence of so-called electronic attacks targeting vital sites in the country. Egypt is one of the African countries most vulnerable to cyber terrorism, which was confirmed by Kaspersky Labs' announcement that Egypt is among the countries that have been exposed to cyber terrorism. Grab the Ransom attack, such as Britain, Germany, Turkey, Japan, China, France, Russia, and the Philippines. [60]

Seventh,: National Measures to Protect Egyptian National Security:

The Egyptian government's procedures for cybersecurity vary, which are divided as follows: [61]

-Legal efforts: Article 31 of the 2014 Egyptian Constitution stipulates that "the security of information space is an essential part of the national security system, and the state is committed to taking the necessary measures to preserve it."

The Arab Agreement to Combat Information Technology Crimes: Egypt was approved to join the Arab Agreement to Combat Information Technology Crimes in 2014, strengthening cooperation between Arab countries to combat electronic terrorism, and "adopting a joint criminal policy aimed at protecting Arab society of information crimes". [62]

The Anti-Information Technology Crimes Law: The issuance of the Anti-Information Technology Crimes Law comes as an important step in the light of Egyptian law, as the law emphasized the "criminalization of illegal electronic practices" that embrace violence and terrorism. According to this law, the punishment is determined according

to the size and nature of the crime. In information crimes, the punishment is considered a deterrent, given its connection to the state's national security. [63]

-Government Efforts: The Egyptian government's executive efforts are represented in developing the National Cybersecurity Strategy (2017-2021), which aims to "prepare a strategy, policies, programs, and plans to secure the critical communications and information infrastructure for all sectors of the state." The most important targeted sectors are the communications and information technology sector, the financial services sector, the energy sector, the transportation sector, the health sector, and sectors that have repercussions and impact on the situation and vital activity in the country, including the following: [64]

- Ministry of Communications and Information : The National Center for "Computer and Network Emergency Preparedness" (CERT-EG) was established in 2009, to confront electronic terrorism, and the center is interested in providing support to the government and financial sector, through technical and field support and submitting technical reports to the competent authorities.

- The "Cyber Security" Council: It was launched in 2014, by a decision of Prime Minister (Former)Ibrahim Mehleb, and is concerned with the security of the communications and information technology infrastructure. The Council is chaired by the Minister of Communications, and the Council aims to develop strategic plans to confront electronic attacks.

- International cooperation: Egypt is keen on international and regional participation in order to enhance cybersecurity, in addition to international cooperation agreements through the Egyptian CERT Center for Cybersecurity. [65]

- Cybersecurity Readiness Index: The Global Cybersecurity Index GCI issued by the International Telecommunication Union shows and measures the preparations made by the Egyptian state through five standards: "the legal standard, the technical standard, the regulatory standard, and the capacity building standard." And the criterion of cooperation, and the ranking that Egypt occupied in the index reflects the effectiveness of the efforts made by the Egyptian government in the field of cybersecurity, which ranked 23rd out of 155 countries in the world. [66]

The Egyptian government has also prepared special programs to deter electronic crimes and limit their spread by employing artificial intelligence tools and techniques and virtual and augmented reality, as cybersecurity has become an important part of the Egyptian security system, and the Egyptian Ministry of Interior has been able to keep pace with technological and communication developments in the world and strive to protect its electronic borders by securing the human element and investigating the working individuals and the extent of their sincerity and loyalty to the security institution in which they work.[67]

The Egyptian government also hosted the Cybersecurity Exhibition and Conference "CAISEC'22" 2022 under the title "Cybersecurity in Times of Crises," in which major companies participated, including: Dell, Microsoft, Cisco, Huawei, Intel,

Orange, Kaspersky, Cyber Force, and Top Tech. At the level of international participation, the Egyptian government is keen to enhance international cooperation in the field of cybersecurity, as it has participated in international and regional forums affiliated with the United Nations, the League of Arab States, the African Union, and the Organization for Economic Cooperation and Development, in addition to signing a number of international cooperation agreements related to Cyber security and threats through the National Center for Computer Emergency Preparedness, and then the most prominent features of international cooperation experiences can be seen through the following points: [68]

- Cooperation with the United Nations: During his meeting with the Secretary-General of the United Nations in 2019, the Egyptian President stressed the importance of intensifying the efforts of the international community to prevent terrorism from exploiting modern technology, and that technological developments have added new dimensions to the phenomenon of terrorism, which has been used against Egyptian state institutions.

- Cooperation with Arab Communications Ministers: During the 37th session of the Council of Arab Communications Ministers in 2015, the Minister of Communications presented a proposal to enhance Arab cooperation on combating cyberterrorism, as Egypt called on countries of the world to join efforts to establish “general principles for building confidence and security in the use of information technology and Communications” through initiatives targeting the following: [69]

Establishing mechanisms to combat cyberterrorism to ensure the preservation of the national security of countries and the safety of their citizens.

Establishing internationally agreed upon foundations among all countries and stakeholders regarding confronting new threats from various sources, especially those that depend on information and communications technology.

Agreeing on fixed terminology and a specific description of cybercrimes, especially those that threaten the security of states.

Eighth,: The Egyptian National Strategy for Securing Cyberspace:

As a result of the multiple risks and threats facing state institutions, Egyptian security institutions have formed electronic warfare units within the main branches of the armed forces and the police and intelligence establishments to respond to rumors and misleading information spread by the Egyptian opposition abroad. The National Cybersecurity Strategy includes the following: [70]

Identifying institutions at risk and raising awareness at all levels - from institutional leaders to ordinary citizens, as people cannot give importance to security without understanding the extent to which their daily activities are at risk. Therefore, the Egyptian government took the initiative to launch national campaigns to increase public awareness, enhance education, training, skills development, and empowering its citizens to become part of the solution.

Identify the necessary resources, arrange them according to the required priorities, focus them on high-value assets, and give priority to appropriate security measures.

Preparing appropriate legal and regulatory frameworks to protect society from cybercrimes, piracy, etc.

The variety of tools used in awareness-raising, including policies, legislation, regulations and other international initiatives in order to increase the level of security and confidence using information and communications technologies.

Improving awareness through continuous monitoring to detect threats that may affect community institutions, and using the latest technologies to detect, repel and contain such threats.

Develop the national capabilities necessary to increase readiness, respond to, and recover from cybersecurity risks when they arise (such as large-scale cyber crises).

Components of the Egyptian National Cyberspace Strategy:

The problem of confidentiality and lack of information arises when dealing with the national strategy of countries in general. Some of them are classified as secret due to their connection to national security capabilities. According to the Egyptian strategy, there are components and tools that support its activities without secrecy, which are as follows: [71]

Strategic political support, which includes awareness of the seriousness of cyber threats and the need to deal with them as a priority and with the utmost seriousness.

Paying attention to advance preparedness, including strategic and operational plans, emergency plans, accidental coordination mechanisms, cadre preparation, and technical and logistical equipment.

Developing the appropriate legislative framework for cyberspace, combating cybercrime, protecting privacy, digital identity, and information security, with the participation of concerned parties and experts in the private sector and civil society organizations.

Guided by relevant international expertise, experiences and programs, while preparing and training law enforcement specialists in judicial and police agencies. [72]

Establishing a regulatory framework and establishing a national system to protect cyberspace security and secure communications and information technology infrastructure, national databases and information systems, government service portals, and government websites on the Internet by preparing and activating “computer and network emergency preparedness and response teams” in vital sectors at the national level.

Encouraging, supporting and developing scientific research and development and supporting cooperation between research bodies and national companies, especially in the field of advanced malware analysis, digital evidence analysis, protecting and securing industrial control systems, and developing devices and systems for securing systems and networks. [73]

Developing the human resources and expertise necessary to activate the cybersecurity system in various sectors, in cooperation and partnership with the private sector, universities, civil society, and relevant international and regional organizations.

Ninth,:Results of the Study:

The results concluded that cyberspace is no longer an isolated issue in the field of information technology, but rather has become a comprehensive legal challenge, as national government institutions need to adopt integrated strategies that meet the requirements of the state's laws and maintain its national security, which requires understanding the implications of various laws. approved by the Egyptian government regarding advanced electronic threats to ensure the protection of its national security.

The results showed the growth of the phenomenon of electronic piracy in Egypt, and this is due to the lack of a department specialized in prosecution, as well as the inability of the concerned administration to follow up the situation effectively, as a result of the lack of technical, financial and human capabilities despite the existence of specialized centers and bodies, some of them are still inactive.

The results indicated an increase in the rates of electronic crimes, which varied between promoting rumors, spreading vice, and terrorist violence, in addition to bullying, fraud, and electronic blackmail, and the growing role of actors, including activists, committees, electronic armies, and non-state actors in the cyber field.

The results of the study revealed the existence of modern threats to Egyptian national security, represented in "cyberwarfare and espionage," which are linked to states, and "cybercrimes and cyberterrorism," which are linked to non-state actors, as cyber threats have crossed the barrier of data, information, and websites to reach infrastructure and vital systems such as nuclear reactors, electricity systems and other sectors that are considered basic pillars of the security of countries.

The results of the study showed that cyberspace is considered one of the components of national security, and that cyberterrorism means committing terrorist acts using information technology systems that represent a threat to national security, and that cybercrimes are crimes related to the computer and the network through cyberspace, criminal activity carried out by using the computer, and illegal work through which computers are used either as a tool or a target, or both.

The results showed the interest of the National Cybersecurity Strategy in Egypt in educational aspects, as Al-Azhar Foundation established what is known as the "Al-Azhar Observatory" in 2015 to follow up and monitor the articles and fatwas issued by terrorist and extremist groups around the world with the aim of responding to them. The results showed the Egyptian government's efforts through a number of precautionary measures to deter cyber threats, through anti-terrorism laws, and the launch of national and regional institutions and bodies specialized in cyber security, including the National Center for Computer and Network Emergency Preparedness, as well as the expansion of training programs to educate government agencies' employees the dangers of Cyber space.

Tenth,: Study Proposals:

Activating operations to monitor vital sites and networks and assessing their strengths and weaknesses while improving cyber defense measures, expanding early warning capabilities in the form of large-scale networks on the one hand, and engaging in

intensive training to raise the efficiency of cyber defense and rapid response teams on the other hand.

Increasing awareness of the danger of cyberterrorism and ways to combat it using the latest technological technologies, while raising the necessary capabilities to develop and implement Egyptian strategies related to combating cyberterrorism.

Developing a comprehensive vision of the most important strategic institutions and bodies whose targeting may result in heavy losses, forcing each of them to develop security plans to defend their systems against any potential attacks, while assessing the needs, human resources, and financial costs of securing each of them.

References:

- [1] Wynne, Michael. Flying and Fighting in Cyberspace, Space Power Journal & Air, fall 2007, pp: 1-11,
- [2] Daniel Colin and Avir Rot Bart. The Proliferation of weapon in cyber : Military and strategic affairs, N01, May 2023: p59 .61. Online e – article:
[http://WWW.INSS.Org.il/upload/Images/System files/ mas5 -1 Eng4-cohen 20 % and 20% Robert](http://WWW.INSS.Org.il/upload/Images/System%20files/mas5-1%20Eng4-cohen%20%20and%20%20Robert%20Libicki,%20Martin%20C.%20Conquest%20in%20Cyberspace%20National%20Security%20and%20Information%20Warfare,%20New%20York,%20Cambridge%20University%20Press,%202022,%20Pp.13-323)
- [3] Libicki, Martin C. Conquest in Cyberspace: National Security and Information Warfare, New York, Cambridge University Press, 2022, Pp.13- 323.
- [4] Dunn Myriam A. , The Internet and the Changing Face of International Relations and Security, Vol. 7, Issue number 1, Procom Ltd., Sofia, Bulgaria, 2001
- [5] Peake ,Adam, Internet governance and the World Summit on the Information Society WSIS)- Prepared for the Association for Progressive Communications (APC), June 2004
- [6] A false sense of security Cybersecurity in the Middle East, Global State of Information (Journal Security, March, p4, 2016
- [7] Brickey, Jonalan ,Capturing a Broad Range of Activities in Cyberspace, CTC Sentinel, Vol.5, No. 8, pp.4-6, 2012.
- [8] Awan, Imran and Blakemore, Brian ,Policing Cyber Hate: Cyber Threats and Cyber Terrorism ,Farnham: Ashgate Publishing, p.43, 2012.
- [9] Howard Philip N. & Samantha Bradshaw, The Global Disinformation Order 2019 Global Inventory of Organized Social Media Manipulation, Computational Propaganda Research Project, Oxford Internet Institute, London: University of Oxford,
<https://demtech.oii.ox.ac.uk/wpcontent/uploads/sites/93/2019/09/CyberTroop-Report19.pdf> ,accessed on 2/08/2021
- [10] Official website of United Nations ,The Charter of the United Nations, 24 October 1945, [https://www.un.org/en/sections/un-charter/introductory-note/index .html](https://www.un.org/en/sections/un-charter/introductory-note/index.html) ,accessed on 06/02/2021
- [11] aklaa, Cherif, Cyber security and the challenges of espionage and penetration of countries through cyberspace, Journal of Law and Human Sciences, University of Algiers 3, Vol. 15, Issue 1, 2022.
- [12] Ben azouz, Hatem, Cyber Security and Cyber Crime in Post-Modern Countries: United States of America-model, Al-Resala Journal for Media Studies, Vol. 6, No. 2, Algeria, 2022
- [13] Messika, Mohamed, Cyberspace and national security challenges for countries, Journal of Legal and Social Sciences, University of Algiers, Issue 1, 2022.
- [14] Gamal, Youssef, Social media Sites as one of the security media platforms in Algeria, Maghreb Journal of Historical and Social Studies, Rabat, Vol 9, No 1, Pp. 208-228 ,2022.
- [15] Tala, Lamia ,Cyber threats and crimes and their effects on the national security of countries, Maalem Journal for Legal and Political Studies, University of Algiers 3, Issue 2, p. 60, 2020.
- [16] Mosa, Hazim, Strategic Vision for Iraqi National Security in Cyberspace: Approach between the security dilemma and performance machinery, Algerian Journal of Legal and Political Sciences, University of the Valley, Algeria, Vol. 57, Issue 5, 2020
- [17] Acho, Fatima Zahraa, The impact of cyberspace on national security in Algeria, Master's Thesis, Kasdi Merbah University, Faculty of Law and Political Science, 2017/2018).

-
- [18] Khalifa, Ihab, Cyberspace to mobilize, Future Studies Unit, Bibliotheca Alexandrina Publications, Egypt, 2014.
- [19] Clarke, Richard, Robert Nick, Cyber war: the second threat to national security, Emirates Center for Political and Strategic Studies, Dubai ,2012.
- [20] Abdel-Sadiq, Adel , Mass proliferation weapons in the cyberspace era, Arab Center for Cyberspace Research, Cairo, October Issue, 2006.
- [21] Ali, Jamal Salama ,Analysis of International Relations, Dar Al-Nahda Al-Arabiya, Cairo.
- [22] International telecommunication Union, ITU-IMPACT establishes first Cybersecurity Innovation Centre for Arab region, Connect World, 19 December 2012, <https://connect-world.com/> ,accessed on 22/06/2021
- [23] Georgetown University Law Library ,International and Foreign Cyberspace Law Research Guide, <https://guides.ll.georgetown.edu/cyberspace> ,accessed on 22/06/2023
- [24] Gamer, Noah ,The intersection of politics and cyber secure ,September 28, 2015. <https://blog.trendmicro.com/the-intersection-of-politics-and-cyber-security/>, accessed on 07/02/2023
- [25] Ramachandran, Ravikumar, Cybersecurity and its Critical Role in Global Economy ,ISACA Now Blog, 23 January,2023.
- [26] WannaCry cyber-attack, available at: www.nao.org.uk/report/investigation
- [27] Heroes of Information Technology, available at the link :www.theregister.co.uk/20/01/2023
- [28] www.darkreading.com/vulne.id/1330845-rat/d/d-a-and-system-controller-safety-its-in-flaw-day-used 2018
- [29] PwC, A false sense of security? Cybersecurity in the Middle East, Global State of Information Security Survey, March 2016
- [30] Muhammad Muhareb , War in Cyberspace, master's Thesis, Al-Najah College, Nabis, p. 86
- [31] Algirde Pipikaite & Others, These are the top cybersecurity challenges of World Economic Forum, 21 Jan 2021,
- [32] Global Cybersecurity Index: <https://www.itu.int/en/ITU.D/Cybersecurity/Pages/GCI.aspx>
- [33] Global Cybersecurity Index GCI , International Telecommunication Union, Switzerland, P.57. 2018,
- [34] Hathaway, Melissa, National Cyber Risk Management, available at: <https://ctm.columbia.edu/people/melissa-hathaway>,2020.
- [35] Jordan, Tim, Cyber power: The Culture and Politics of Cyberspace and the Internet". Rout ledge, pp: 160-254,2000.
- [36] Kelly A. Gable, Cyber-Apocalypse Now: Securing the Internet against Cyberterrorism and Using Universal Jurisdiction as a Deterrent", Vanderbilt Journal of Transnational Law, Vol.43, no. 1, p.33,2010.
- [37] Grant, Rebecca, Victory in Cyberspace, The Eaker Institute, the policy and research arm, The Air Force Association of US, October 9, 2017.
- [38] Fathi, Ahmed ,How the Brotherhood spreads :cyber-terrorism" in Egypt, Al-Ain News,2023. available at: <https://shorturl.at/cpqtM>
- [39] Ezzi, Alia, The Brotherhood and digital media, Trends Center for Research and Studies, available at: <https://trendsresearch.org/research.php?id=294>
- [40] International Multilateral Partnership Against Cyber Threats (IMPACT), https://en.wikipedia.org/wiki/International_Multilateral_Partnership_Against_Cyber_Threats ,accessed on 11/05/2023
- [41] Cyber Security Intelligence ,Cyber Warfare Is The New Frontier NATO treaty warfare army hackers, <https://www.cybersecurityintelligence.com/2020/12/15> ,
- [42] Kaplan, J. , Meeting the cybersecurity challenge, McKinsey Quarterly,2011
- [43] The Egyptian state's efforts to combat terrorism, Ministry of Foreign Affairs report, 2021, available at: <https://shorturl.at/wPR13>
- [44] Gabriel Weimann, Terrorism in Cyberspace: The Next Generation (New York, NY: Columbia University Press, , p23. 2015.

-
- [45]Kristen Eichenseh, Today's Revolution: Cybersecurity and the International Order, Lawfare, February 8, 2018,, <https://www.lawfareblog.com/todays-revolution-cybersecurity-and-international-order> .Accessed on 09/01/2023
- [46]Home office, Cyber Crime Strategy, March 2010, p9, available: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228
- [47]Wigan Council, Cyber terrorism, Available online: <https://shorturl.at/ewRS7>, Accessible on August 27, 2023.
- [48]Daily News Egypt, Kaspersky Tackles 13 Million Cyberattacks in Egypt During 1Q 2023, Daily News Egypt, May 8, 2023, Available online: <https://shorturl.at/tGW18>, Accessible on September 25, 2023.
- [49] Tala, Lamia ,Cyber threats and crimes and their effects on the national security of countries, Maalem Journal for Legal and Political Studies, University of Algiers 3, Issue 2, p. 60, 2020.
- [50]Murat Dogrul, Adil Aslan, Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism, 3rd International Conference on Cyber Conflict, Tallinn, Estonia, 2011, p. 10.
- [51]Cyber Security Intelligence ,Cyber Warfare Is the New Frontier NATO treaty warfare army hackers, <https://www.cybersecurityintelligence.com/>
- [52] Vavra, Shannon, The world's top cyber powers ,Axios, Aug 13, 2017 <https://www.axios.com/the-worlds-top-cyber-powers-1513304669-4fa53675-b7e6-4276-a2bf-4a84b4986fe9.html>, accessed on 22/05/2023
- [53]Kristen Eichenseh, Today's Revolution: Cybersecurity and the International Order, Lawfare, February 8, 2018,, <https://www.lawfareblog.com/todays-revolution-cybersecurity-and-international-order> .Accessed on 09/01/2023
- [54]Alshalan. A, Cyber-crime and Victimization. Unpublished Ph.D. Dissertation in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy in Sociology in Department of Sociology, Anthropology and Social Work Mississippi State University.2006
- [55]League of Arab States, Arab Convention to Combat Information Technology Crimes, , Cairo, p. 1, December 21, 2010
- [56] Fathallah, Mahmoud Ragab, Explanation of the Law on Combating Information Technology Crimes According to the New Egyptian Law, Alexandria: New University House.2018.
- [57]National Cybersecurity Strategy (2017-2021), Egypt, Presidency of the Council of Ministers, Supreme Council for Cybersecurity, p. 7.
- [58] Abdel Dayem, Heba, "Cyber Attacks", National Investment Bank, Cairo, p. 9,2017.
- [59] Hower, Sara Kathleen Uradnik, Cyberterrorism, 1st ed. (Santa Barbara, CA: Greenwood,), pp142–146, 2011.
- [60]Global Cybersecurity Index GCI (2018), International Telecommunication Union, Switzerland, P.57, 2018.
- [61]Cybersecurity in Egypt, previous reference, available at <https://www.sis.gov.eg/Story/258293/>
- [62]League of Arab States, Arab Convention to Combat Information Technology Crimes, , Cairo, p. 1, December 21, 2010
- [63] Hashem, Sherif, "Towards a National Cybersecurity Strategy," Presidency of the Council of Ministers, Supreme Council for Cybersecurity, p. 8,2019.
- [64]Cybersecurity in Egypt, previous reference, available at the link : <https://www.sis.gov.eg/Story/258293/>
- [65]<https://www.sis.gov.eg/Story/258293/>
- [66] Hathaway, Melissa, National Cyber Risk Management, available at: <https://ctm.columbia.edu/people/melissa-hathaway>
- [67]Cybersecurity in Egypt, previous reference, available at <https://www.sis.gov.eg/Story/258293/>
- [68]Global Cybersecurity Index GCI , International Telecommunication Union, Switzerland, P.57,2018.
- [69]<https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2019/cybersecurity-and-its-critical-role-in-global-economy> ,accessed on 29 June 2021

[70]Cybersecurity in Egypt, previous reference, available at <https://www.sis.gov.eg/Story/258293/>

[71]Cybersecurity in Egypt, previous reference, available at <https://www.sis.gov.eg/Story/258293/>

[72]United Nations Office on Drugs and Crime (2023) Comprehensive Study on Cybercrime. United Nations, May 2023

[73]<http://www.inquiriesjournal.com/articles/627/cyber-terrorism-and-ir-theory-realism-liberalism-and-constructivism-in-the-new-security-threat> ,accessed on 16/12/2023