Dr. Asmaa Gaber Mahran

Assistant Professor of Crime Sociology- Faculty of Arts - Assiut University

Social Implications and Risks of Cyber Crimes and Attacks on Digital Security and Countermeasures in Light of Egypt's Vision 2030

Introduction:

A survey conducted by the Organisation for Economic Co-operation and Development (OECD) on the digital economy revealed that governments ranked security as the second highest priority area, and privacy as the third among 31 possible policy priority areas. In the same vein, consumers are increasingly concerned about privacy in the digital environment. A 2014 study by CIGI-IPSOS on internet security and trust among internet users in 24 countries showed that 64% of participants are more concerned about privacy than they were a year before (1).

Despite the difficulty of measuring them quantitatively, security incidents appear to be increasing in complexity, frequency, and impact(2). Over the past decade, critical activities have increasingly faced digital security threats, a trend that is accelerating with the current digital transformation. The anticipated benefits of smart cities, digitally enhanced energy grids, and healthcare are driving the adoption and utilization of technologies such as big data, artificial intelligence, Internet of Things (IoT) devices, and 5G networks. Although these technologies are considered emerging, they add complexity to the digital ecosystems supporting critical activities by expanding the attack surface for operators of critical activities. This expansion is proportional to the increasing amounts of data, devices, software, and network infrastructures they have to manage, which cannot be considered entirely secure (3).

The likelihood that digital security incidents could lead to physical damage is no longer theoretical. Cybersecurity attacks have destroyed nuclear centrifuges in Iran, caused immense physical damage to a German steel plant in 2014, and led to power outages in Ukraine in 2015 and 2017. Moreover, the NotPetya incident in 2017 demonstrated that cybersecurity attacks could significantly disrupt operations and supply chains for several days in sectors such as global container logistics (Maersk) and pharmaceutical production (Merck). In 2021, a cyberattack forced the Colonial Pipeline Company to shut down the largest pipeline in the United States for six days, resulting in fuel shortages across the East Coast (4).

Study Problem:

People have moved from the physical world to the virtual world, and so has crime. We can imagine the extent of interactions taking place in the virtual world, whether personal, institutional, cultural, or in the business and service fields. It is essential to note that cyberspace has produced new types of crime called cyber crimes by creating new opportunities for criminals. Cyberspace criminals can browse the internet and commit unique crimes in this space. These features form transformative keys, namely:

1- Globalization: enabling offenders to exploit new opportunities by crossing traditional boundaries.

2- Distributed Networks: creating opportunities for forming victims.

3- Panopticism and Synopticism: allowing offenders to remotely humiliate their victims.

4- Data Trails: creating opportunities for identity theft. Moreover, the number of cybercrime victims is on the rise, especially those suffering financial losses, threats, or harassment due to the increase in internet users. Cybercrime represents a new field of research in criminology [(5)].

From the above discussion, it is clear that the current study's problem lies in answering the main question:

What are the social implications and risks of cyber crimes, attacks, and threats on digital security, and what are the countermeasures in light of Egypt's Vision 2030?

This main question gives rise to several sub-questions:

A. What are the generations of cyber attacks?

B. What is the nature and forms of cyber crimes and attacks?

C. Who are the threat actors in the cyber environment?

D. What are the social risks of cyber crimes and attacks on digital security?

E. What are the mechanisms and efforts of the Egyptian state in countering cyber attacks in light of Vision 2030?

F. What is the proposed framework for addressing the social risks of cyber crimes and attacks on digital security in Egypt?

Significance of the Study:

- ***Scientific Significance:***

A- The scientific significance of this study lies in its attempt to shed light on a new field in social sciences, specifically the sociology of crime. According to the researcher, this study is the first Arabic study to address digital security from a sociological perspective, which we hope will contribute to opening new future horizons in sociological studies.

B- It adds to the theoretical heritage by studying a new concept, digital security, which is different from information security.

- ***Practical Significance:***

Observing the social impacts of cyber crimes and attacks on digital security is important for individuals to raise awareness of their risks and how to confront them. It is also crucial for officials and decision-makers to develop strategies to combat these threats and enhance both defensive and offensive capabilities, as they pose a serious threat to both individuals and the state as a whole.

Objectives of the Study:

The primary objective of the current study is to examine the social implications and risks of cyber crimes, attacks, and threats on digital security and to identify countermeasures in light of Egypt's Vision 2030. From this general objective, the following sub-objectives emerge:

A. Identify the generations of cyber attacks.

B. Determine the nature and forms of cyber crimes and attacks.

C. Identify the threat actors in the cyber environment.

D. Reveal the societal risks of cyber crimes and attacks on digital security.

E. Observe the mechanisms and efforts of the Egyptian state in countering cyber crimes and attacks in light of Vision 2030.

F. Develop a proposed framework to address the social risks of cyber crimes and attacks on digital security in Egypt.

Study Methodology:

The current study will rely on the systems analysis methodology developed by David Easton for analyzing social phenomena and systems. This involves breaking down the phenomenon into its elements as inputs, studying the impact of variable factors on them as processes, and then examining the outputs and comparing them to the inputs through what is known as feedback to study the relationship between cause and effect [6].

Accordingly, the study topics will be divided based on this methodology as follows:

- ***A. Inputs:*** These will include the study concepts such as cyber crimes, cyber attacks, and digital security.
- ***B. Processes:*** These will include the study and analysis of the objectives related to the study's subject, which involve identifying the generations of cyber attacks, the nature and forms of cyber crimes and attacks, the threat actors in the cyber environment, the social risks of cyber crimes and attacks on digital security, and the efforts and mechanisms of the Egyptian state in countering cyber crimes and attacks in light of Vision 2030.
- ***C. Outputs:*** These will include the developed methodology that the study aims to reach as a proposed framework or new methodology for countering the risks of cyber crimes and attacks on digital security.

The Sociological Perspective on Studying Digital Security:

1. Risk Society Theory to Monitor the Implications of Cyber Crimes on Digital Security:

German sociologist Ulrich Beck is the founder of this theory and the first to introduce the concepts of risk and the global risk society. The risk theory addresses the increasing presence of uncertainty in the face of societal changes. The industrial society has given way to a technological and information risk society, often referred to by postmodern theorists as the "world of chaos," where stable life patterns disappear[7]. The global risk society represents a unique period in history capable of self-destruction through technology[8]. Consequently, digital security faces numerous risks due to the digital revolution, which has led to the evolution of cyber crimes and attacks, resulting in the loss of individuals' cultural privacy and the appropriation of digital information belonging to individuals, institutions, and states [9].

2. Structuration Theory to Monitor the Components of Digital Security:

Structuration Theory by Anthony Giddens offers a theoretical vision for resolving the social issue of the structure-agency problem. According to this theory, digital and cyber security practices are among the primary manifestations of structuring the social framework. The key issues highlighted by Anthony Giddens are [10]:

A. The structuring process involves the active participation of agents and successful daily practices.

B. Structure imposes limits on human action while also facilitating it, known as the "duality of structure."

C. Structure is shaped through the interaction of meanings, norms, and power.

D. Structure is formed through the skilled performance of members, considering space and time.

Thus, the actors, being the perpetrators of cyber crimes and attacks, negatively impact and reshape the social structure according to their dual vision through repeated criminal practices. They are a potent force in the digital space due to their destructive power and act based on specific beliefs and various methods, leading to a range of harmful social risks for individuals and society as a whole.

The study includes the following elements:

1. **The conceptual framework of the study.**
2. **Generations of cyber attacks.**
3. **Patterns of cyber crimes and attacks.**
4. **Types of threat actors in the cyber environment (categories of cyber attackers).**
5. **Social risks of cyber crimes and attacks on digital security.**
6. **Mechanisms and efforts of the Egyptian state in countering cyber crimes and attacks in light of Egypt's Vision 2030.**

7. Criteria and proposed model for addressing the social risks of cyber crimes and attacks on digital security in Egypt.

8. Study results and recommendations.

Firstly: Conceptual Framework of the Study:

1. The Concept of Cyber Crime:

Cybercrime involves a limited number of acts that threatens the confidentiality of data or computer systems and their availability. These acts, carried out using computers, aim to achieve personal or financial gains or cause harm, including crimes related to identity and computer content. They all fall under a broader scope of cybercrime terminology, which cannot easily be adapted to fit comprehensive legal definitions. This necessitates defining and identifying the core acts that constitute cybercrime. Still, defining cybercrime may not be as crucial for other purposes, such as determining the jurisdiction of investigative authorities and international cooperation, focusing on electronic evidence related to any crime is preferred over a broad and artificial composition of "*cybercrime*" (11).

In a broader sense, cyber (electronic) crimes refer to ***"any illegal behavior in which a computer or the internet is used as a tool, target, or both. This illegal behavior involves the use of computing devices such as smartphones, tablets, personal digital assistants (PDAs), and other independent or networked computing devices as a tool or target for criminal behavior committed repeatedly by individuals with destructive and criminal behavior for a variety of reasons, including revenge, money, or adventure."*** According to the Oxford Dictionary, the term cyber crime refers to ***"criminal activities carried out by means of computers or the internet."*** Cyber crime is also defined as ***"criminal activity that occurs on or via computer or the web or any other recognized technology."*** Thus, cyber crime can be summarized as ***"those types that are a crime of a kind, but in which the computer is a thing or subject of the behavior that constitutes a crime"*** (12).

2. The Concept of Cyber Attack:

Cyber attacks occur within a broader context—traditionally referred to as information operations or information warfare—that integrate the core capabilities of electronic warfare, psychological and computer networks, military deception, and security operations, coordinated with specific support and related capabilities. Definitions of cyber attacks have varied among legal and technical specialists, with one of the most significant definitions being that cyber attacks are ***"actions taken by states to penetrate the computers of another state or states to cause damage or disruption"*** (13).

Cyber attacks are also defined as ***"actions that undermine the capabilities or functions of the information network by exploiting vulnerabilities, thereby enabling the attacker to manipulate the system."*** They are also defined as ***"the deliberate exploitation of technology-based computer systems and networks through malicious software"*** (14).

We can distinguish and highlight the differences between cyber crime, cyber warfare, and cyber attacks as follows:

Cyber Crime (Electronic Crime): These are cyber actions undertaken exclusively by non-governmental attackers, executed through a computer system, constituting a violation of criminal law.

Cyber Attack and Cyber Warfare: The purpose of a cyber attack is to destroy and disrupt the operation of a computer network for political or security purposes. The effects of a cyber attack are similar to those of an armed attack or a cyber action occurring in the context of an armed assault (15).

3. The Concept of Digital Security:

International and national industry standards often include definitions of digital security. It should be noted that there is no universally accepted global definition or consensus on the precise scope of this term. Within the United Nations context, inspectors have observed that there are no guidelines within the framework of joint forums among relevant agencies recommending consensus on a specific definition to be trusted by the system. Furthermore, organizational regulatory frameworks do not systematically attempt to impose a definition of digital security.

According to the International Telecommunication Union (ITU), digital security is defined as: ***"A set of tools, policies, security concepts, assurances, guidelines, risk management approaches, procedures, training, best practices, and technologies that can be used to protect the cyber environment and organizational assets and users. Organizational assets and users include interconnected computing devices and personnel, infrastructure, applications, services, and stored or transmitted information within the cyber environment. Cybersecurity aims to ensure the achievement and maintenance of security properties of organizational assets and users against relevant security risks in the cyber environment. The general security objectives include availability, safety (including reliability and non-repudiation), and confidentiality"*** (16).

Meanwhile, the European Cyber Security Agency, in its first legislation issued in 2001, defined digital security as: ***"The ability of an information system to resist unauthorized access, or unforeseen incidents targeting data in transit or at rest within an interoperability framework"*** (17).

Similarly, the Herdo Center for Digital Expression Support defines digital security as: ***"How to effectively use the Internet without being exposed to any threats, risks, or surveillance that threaten the privacy and confidentiality of information"*** (18).

Regarding the concept of digital security, it serves as a tool for enhancing cooperation in combating various forms of cyber crimes and confronting their risks. It is worth noting that among the countries that have focused on the concept of digital security, the United Kingdom ranks first globally according to the Global Cybersecurity Index (GCI) issued by the International Telecommunication Union (ITU), followed by the United States. Among Arab countries, Saudi Arabia ranked first, followed by the Arab Republic of Egypt and Qatar (19).

Secondly: Generations of Cyber Attacks:

These can be summarized as follows (20):

First Generation (1989-1990): In the late 1980s, intruders launched viral attacks on used computers, prompting affected users and private companies to develop antivirus (AV) products focusing on signature information.

Examples of first-generation cyber attacks include:

- (1982 - ELK Cloner): The world's first computer virus.

Second Generation (1995): In the mid-1990s, rapid-propagating worm attacks emerged directly from the widespread internet, compelling companies to build perimeter defenses to repel attackers.

Examples of second-generation cyber attacks include:

- (Morris Worm - 1988): One of the first computer worms, resulting in criminal charges in the United States under fraud and computer abuse laws.
- (Melissa - 1999): The first mass-mailing macro virus.

Third Generation (2005): During the early years of the new century, criminals began exploiting software vulnerabilities that could impact businesses utilizing them. This period also witnessed the transition of motives from experimentation to profit, initially through the use of botnets for distributing spam.

Examples of third-generation cyber attacks include:

- (2000 - I Love You): A worm affecting tens of millions of Windows computers.
- (2003 - SQL Slammer): Service denial to 75,000 hosts.

Fourth Generation (2010): During the first quarter of the previous decade, there were no signs of targeted attacks. Discussions about the absence of clear evidence regarding weapons of mass destruction led citizens to heed the phrase "the invisible hidden one" coined by then-U.S. Secretary of Defense Ronald Rumsfeld.

Examples of fourth-generation cyber attacks include:

- (2010 - Stuxnet): A state-sponsored development targeting SCADA systems in critical infrastructure, including Iran's nuclear program.
- (2016 - DYN Attack): A massive Distributed Denial of Service (DDoS) attack on the primary DNS provider.

Fifth Generation (2017): Starting in 2017, large-scale, widely financed attacks by some governments began to be executed by numerous companies. These cyber crimes have their own internet networks and specific assurances.

Examples of attacks from the fifth wave include:

- (2017 - WannaCry): A major ransomware attack affecting 200,000 computers in 150 countries.

Thirdly: Patterns of Cyber Crimes and Attacks:

1. Patterns of Cyber Crimes:

Cyber crimes have emerged and evolved to become one of the fastest-growing threats in the world of crime, making it challenging to determine the extent of the spread of these criminal activities. Classified cyber crimes include [21]:

- Unauthorized access to computer data.
- Intrusion into information systems.
- Misuse of devices or software.
- Financial crimes.
- Sexual exploitation of minors.
- Violations of intellectual property rights in digital works.
- Crimes involving credit cards and electronic money.
- Crimes affecting personal information.
- Racial crimes and crimes against humanity through information means.
- Crimes involving gambling and drug trafficking through information means.
- Cyber crimes against the state and public safety.
- Information encryption crimes.

2. Types of Cyber Attacks:

Cyber attacks can be classified into the following categories [22]:

A. Attacks on the Internet Network:

These attacks occur on websites or web applications, and examples include:

- Injection attacks: such as SQL injection, XML injection, code injection, and registry injection, where data is injected into a web application to manipulate its processing and retrieve desired information.
- DNS spoofing.
- Phishing attacks, including Spear phishing, whaling, Smishing, Vishing, Email Phishing, and SEO Poisoning.
- Denial-of-Service attacks (DRDOS/DDOS/DOS).
- Man-In-The-Middle attacks, including Wi-Fi eavesdropping, email or SSL hijacking, IP or HTTPS or DNS spoofing.

B. System-based Attacks:

These attacks aim to compromise computer systems or networks, and examples include:

- Viruses.
- Worms.
- Trojan horses.
- Backdoors.
- Bots.

Furthermore, Egypt's National Cyber Security Strategy (2023-2027) revealed a significant increase in cyber attacks in previous years, causing substantial economic losses globally. This poses a major burden on national budgets. Additionally, these attacks have led to other losses such as disruptions of critical services and damage to the reputation of companies and individuals. The strategy also identified diverse sources of cyber threats, including cyber crime, cyber warfare, terrorism, insider threats, and amateur threats [23]:

- Cyber Crime:

Cyber crime primarily involves the development and dissemination of malicious software for financial gain or piracy, aiming to steal, damage, or manipulate data and networks. These attacks have become increasingly aggressive and widespread worldwide, exemplified by the rising use of Ransomware and Denial-of-Service (DDOS) threats for purposes of sabotage or extortion.

- Cyber Warfare:

Cyber warfare involves threats initiated by states or state-sponsored groups targeting critical sectors in other countries, such as energy, communications, banks, and others, for espionage, political and strategic gains, or purely for destructive purposes. Many countries openly declare possessing cyber offensive capabilities for self-defense against such threats.

- Terrorism:

Despite terrorists' limited cyber capabilities currently, future projections indicate increasing potential for significant damage, placing cyber terrorism on the map of potential threats.

- Insider Threats:

With the increasing use of information technology within organizations, the risks from authorized employees unintentionally or intentionally exploiting information systems are growing. These employees can become sources of institutional threats by stealing sensitive data, leading to substantial financial losses or damaging the organization's reputation. Employees may unknowingly expose sensitive institutional data to risks through cyber attacks like Phishing or Social Engineering.

-Amateurs (Kiddies Script):

These individuals possess limited cyber skills but use prepared programs with high destructive capabilities, targeting vulnerabilities in institutional information systems when encountered.

Fourthly: Types of Threat Actors in the Cyber Environment (Cyber Attackers Categories):

The main types of threat actors in the cyber environment are as follows [24]:

- ***Computer Hackers:***

Individuals or groups who penetrate networks to cause disruption, harm, or chaos, often driven by motives of fame or challenge.

- ***Hacktivists:***

These actors have specific motivations, viewing their activities as a form of civil disobedience or a means to express political or ideological views.

- ***Cyber Criminals:***

Actively engaged in criminal activities facilitated by cyber means (common crimes such as fraud, theft, extortion, etc.) using computer tools, or involved in criminal activities entirely dependent on the cyber space, such as spreading viruses or malware.

- ***Industrial Espionage:***

A sub-category of organized crime with specific goals of obtaining trade secrets, economic espionage, or sabotaging competition.

- ***State-Sponsored Groups:***

Highly advanced entities with substantial resources, often difficult to detect, trace, or attribute their activities. They may pursue complex and often indirect goals, directly supported by governmental or military entities or indirectly funded by them.

- ***Insiders:***

Actors who pose a threat from within an organization, not necessarily due to their contractual relationship with the concerned organization, but due to internal risks. This category may include disgruntled employees, poorly trained employees, contracted service providers with inadequate training, among others.

Fifthly: Social Risks of Cyber Crimes and Attacks on Digital Security:

Cyber crimes (electronic) have caused harm to citizens, companies, and governments in several ways, such as the loss of sensitive business information, loss of customer trust, loss of intellectual property, business losses, and more. The Center for Strategic and International Studies has mentioned that the annual cost borne by the global economy due to cyber crime incidents exceeds $400 billion. The impacts of cyber crimes will gradually increase with the growth of online business functions and as more companies and customers worldwide connect to the internet. Additionally, cyber crime affects employment rates in advanced countries, where research results have shown that losses from cyber crime can potentially impact up to 200,000 American jobs, representing nearly a third of the decline in employment. In 2014, 3,000 companies in the United States experienced breaches, and Brazil incurred $1.4 billion in damages due to cyber attacks, as over 45% of Brazilians use the internet. In 2013, France lost $5.19 million due to cyber attacks and faced 1,900 cyber attacks since the terrorist attack in 2014. About 91% of businesses in the United Kingdom and 31% of households have internet access. The estimated cost of cyber crimes in the UK is approximately $27 billion [25].

Based on this, the International Telecommunication Union (ITU) report in 2010 on the social dimensions of digital security stated that the digital revolution has changed business dealings and government operations, and globalization and technological advancement have weakened infrastructure, thereby making it a potential target for terrorist attacks. Countries face real risks, and criminals exploit vulnerabilities in precise information systems to disrupt critical infrastructure and national security threats [26].

The main social risks of cyber crimes and attacks on digital security include:

1. Increase in emerging crime rates and resulting losses:

On December 23, 2015, hackers attacked Ukraine's power grid and disabled remote control systems used in substation facilities, leaving people and the western part of the country without electricity for several hours. The Ukrainian Security Service (SBU) blamed the Russian government for the cyber attack, a claim later supported by malware analysis from private computer security firms. This Ukrainian breach was the first publicly acknowledged case of a cyber attack successfully causing a power outage and is just one of thousands of cyber activities occurring alongside physical combat in Ukraine [27].

Given that consumers increasingly rely on computers, networks, and stored information, the risk of exposure to cyber crimes is high. Survey results have shown that up to 80% of surveyed companies admitted to financial losses due to computer breaches, estimated at $450 million. Approximately 10% involve financial fraud, with new attacks affecting computer system confidentiality, integrity, and availability, ranging from personal information theft to denial of service attacks [28].

Aligning with this, over the past fifteen years, numerous issues have affected the transition from information security to digital security, such as increased internal threats like WikiLeaks internal leaks, data breaches, and insider threats. Emerging technologies, specifically external-oriented digital technologies facilitating communication, cognitive technologies, artificial intelligence, mobile phone technology, and social media, have also increased external threats like malware, ransomware, data breaches, interconnected devices, cyber warfare, and state-sponsored attacks. For instance, Ponemon Institute estimated direct costs of data breaches in 2017 amounted to $3.62 million USD [29].

Moreover, police departments nationwide have reported an increasing number of fraud and grand theft incidents in recent years, coinciding with the national trend of increased computer and online business use. In 2004, cyber crime generated higher returns than drug trafficking, and this trend is expected to grow further with expanding technology use in developing countries. Results from 2011 indicated that over 74 million individuals in the United States were victims of cyber crimes in 2010, resulting in financial losses estimated at $32 billion. Sixty-nine percent of adult internet users fell victim to cyber crimes, translating to one million cyber crime victims daily. Many people believe cyber crime involves crimes related to conducting business online [30].

2. Targeting Vital Sectors:

The ransomware program Wannacry had significant impacts on services worldwide, such as the National Health Service in the United Kingdom, where Renault halted production in factories across France, Deutsche Bahn faced issues with train line displays at stations, and Maersk experienced severe container traffic disruptions globally [31].

Examples of destructive cyber attacks also include the famous cyber attack on the colonial pipeline in 2021, which directly led to gas flow interruptions throughout the United States. On the night of September 9, 2020, a ransomware attack struck the systems of the University Hospital Düsseldorf, a major hospital in southern Düsseldorf. Ransomware programs are a form of malware that prevents users from accessing their files, often by encrypting data until a ransom is paid. The hospital's computer network spread the attack, encrypting thirty servers and rendering them inoperable. Patient data became inaccessible, and many Wi-Fi connected medical devices were unavailable, forcing the hospital to halt operations for several weeks while systems were repaired. Concurrently, the attackers demanded a substantial ransom to regain access to the locked computer systems. Upon police notification, the perpetrators claimed the attack inadvertently extended to the local hospital (32).

It's evident from the above that cyber crimes and attacks directly target critical systems and sectors of nations for extortion and personal gain.

3. Destruction of Infrastructure and Targeting National Security:

Cyber warfare does not only target military equipment and systems but also critical societal infrastructure, including smart networks, surveillance networks, and Supervisory Control and Data Acquisition (SCADA) systems that enable operation and self-defense. Cyber conflict can have life-threatening consequences if information infrastructures are corrupted. The ITU-2017 report at the Global Communications Development Conference emphasized the necessity for secure telecommunications and information technology infrastructure, enhancing infrastructure development and services, including building trust and security in communications and information technology usage. Societies face severe economic and social losses if their communication networks or other infrastructure are attacked or disrupted. Technological advancements will exacerbate these losses if sufficient attention is not given to security and infrastructure (33).

One of the fundamental documents for understanding the impact of attacks on infrastructure on societies is the Strategic Bombing Survey conducted by the United States during and after World War II. Britain and America deployed thousands of heavy bombers that dropped millions of tons of high explosives on Germany to paralyze its infrastructure, destroy its industrial base, and break the population's will to continue the war. Early air warfare theorists anticipated that such attacks would cripple the target, and with the escalating pace of air attacks, Germany could not prevent the deterioration and collapse of its economy (34).

4. Digital Identity and Private Data Theft:

Digital identity theft is one of the most dangerous crimes threatening internet users and the future of electronic services. Personal data of users can be stolen with the intent of identity theft, seizing their properties and funds, or using their identity in suspicious or illegal transactions. Identity thieves often utilize information already available on the internet, especially on social and professional networking sites, open databases, national information repositories, government service networks, social security services, healthcare networks, e-commerce websites, virtual markets, electronic payment networks, ATMs, and stock exchanges. Furthermore, tools and systems used in electronic transactions can also be subject to theft or sabotage, posing significant risks to user interests and the future of electronic services. Extended attacks can impact the national financial sector as a whole. Private data of public institutions and companies are vulnerable to theft, resulting in severe financial and reputational losses, affecting their clients and intellectual assets, potentially harming the national economy (35).

Sixth: Mechanisms and Efforts of the Egyptian State in Combating Cyber Crimes and Attacks in Light of Egypt Vision 2030:

The Global Cybersecurity Index (GCI) issued by the International Telecommunication Union revealed that Egypt ranked 23rd globally out of 193 countries. Additionally, Egypt ranked first globally in the competitiveness of the internet and telephone sectors in 2021 according to the Global Knowledge Index. Moreover, Egypt improved its ranking by 3 positions in the Government Readiness for Artificial Intelligence Index issued by the Oxford Group, reaching 62nd place compared to 65th in 2022 (36)..

Efforts and mechanisms of the Egyptian state in cybersecurity and its strength in combating cyber crimes and attacks can be highlighted as follows:

1- Egyptian National Legislation:

- Egyptian Constitution:

Article 31 of the Egyptian Constitution, as amended on April 23, 2019, stipulates that "the information space is an integral part of the economic and national security system. The state is committed to taking necessary measures to preserve it as regulated by law." (37).

- Law on Combating Information Technology Crimes (Law No. 175 of 2018):

For the first time, the law criminalizes "illegal cyber practices" such as creating websites that incite terrorism, cyber forgery, and others. According to this law, penalties are determined based on the scale and nature of the crime. In cases of information technology crimes, severe penalties are imposed due to the serious repercussions on national security, in addition to other penalties related to cyber intrusion, forgery, and more (38).

- Law No. 94 of 2015 on Combating Terrorism:

This comprehensive law addresses terrorism and its financing objectively and procedurally, incorporating necessary measures for legal confrontation against terrorism with efficient procedures and deterrent penalties. The provisions of this law draw from decisions of the Security Council, international and regional conventions in combating terrorism. The law prescribes the same punishment for attempting to commit a terrorist crime or inciting it, and it regulates freezing funds and prohibiting their disposal. Specialized courts are designated for misdemeanors, felonies, appeals, and disputes related to terrorism crimes (39).

2- Strategic Interventions:

A- National Strategy for Artificial Intelligence:

Egypt launched the National Strategy for Artificial Intelligence to utilize this technology in supporting the achievement of sustainable development goals, as well as playing a leading role in facilitating regional cooperation in the African and Arab regions. This initiative reflects Egypt's commitment to engaging with the advancements of the digital age, where technological developments continue to evolve daily (40).

B- National Cybersecurity Strategy (2017-2021):

The Supreme Cybersecurity Council, under the auspices of the Prime Minister's Office and chaired by the Minister of Communications and Information Technology, launched the National Cybersecurity Strategy (2017-2021). Its strategic goal is to confront cyber risks, enhance trust in communication and information infrastructures, and secure them to create a safe and reliable digital environment for Egyptian society across various sectors. This effort aligns with the state's efforts to support national security and the development of Egyptian society (41).

C- Government Cloud Computing Strategy:

The Government Cloud Computing Strategy aims to improve government efficiency and performance by delivering optimal value through enhanced operational efficiency and faster response to integrated needs. The cloud computing model supports government agencies needing to provide highly reliable and innovative services despite resource constraints (42).

D- Launch of the Five-Year National Cybersecurity Strategy (2023-2027):

The Supreme Cybersecurity Council, under the Prime Minister's Office and chaired by the Minister of Communications and Information Technology, launched the Five-Year National Cybersecurity Strategy (2023-2027). The importance of having a national cybersecurity strategy is twofold: firstly, to address the increasing number and sources of cyber incidents, and secondly, to create market opportunities for the Egyptian market through building human capital and developing a national industry that contributes to increasing the Gross Domestic Product (GDP) (43).

3- Establishment of National Centers and Specialized Councils:

A- National Center for Computer and Network Emergency Readiness:

Established in 2009 to counter the threat of cyber terrorism and other cyber threats, this center specializes in providing support to both government and financial sectors through technical and field support. It delivers technical reports to relevant authorities to protect the national information infrastructure, especially in the sectors of information technology, communications, and finance. A highly specialized team operates around the clock to monitor cybersecurity, respond to incidents, conduct digital forensic analysis, analyze malware, and perform reverse engineering. Its primary goal is to enhance the security of Egypt's communication and information infrastructure through proactive measures, information gathering, analysis of security incidents, coordination, and mediation among relevant parties in resolving these security incidents. The center also collaborates internationally with various teams involved in computer and network emergency response in other countries [44].

B- Egyptian Computer Emergency Response Team (EG-CERT):

Established by the National Telecommunications Regulatory Authority in April 2009, EG-CERT operates with a team of sixteen specialists providing 24/7 technical support to protect critical information infrastructures. Since 2012, EG-CERT has been supporting various entities across IT, telecommunications, banking, and governmental sectors to combat cybersecurity threats, including Distributed Denial of Service (DDoS) attacks. Its primary mission revolves around providing early warning systems against malware and widespread electronic attacks targeting Egypt's critical information infrastructure [45].

C- Establishment of the Supreme Council for Securing Telecommunications and Information Infrastructure (National Cybersecurity Council):

Established on December 16, 2014, to protect and secure telecommunications and information technology infrastructures, the National Cybersecurity Council aims to develop strategic plans to counter cyber attacks. It supervises the implementation of national strategies to confront cyber threats, regularly updating these strategies. Additionally, the Executive Office and Technical Secretariat of the National Cybersecurity Council oversee the execution of council activities and plans in line with defined strategies and policies. The Technical Secretariat conducts technical studies requested by the council and its executive office, organizes periodic national awareness campaigns on cyber threats across various sectors, facilitates workshops and courses to raise sector-specific cybersecurity awareness, and develops specifications for secure information exchange systems related to securing state information infrastructures [46].

Seventh: Standards and Proposed Model for Addressing Social Risks of Cyber Crimes and Attacks on Digital Security in Egypt:

1- Proposed Standards for Addressing Social Risks of Cyber Crimes and Attacks on Digital Security:

First Standard: Development of Cyber Security Laws and Regulations:

Addressing cyber crimes and threats requires the establishment of legal frameworks covering all types of cyber crimes and ongoing threats. This includes legislations and regulations to safeguard individuals' rights in the digital space, secure their personal data, and raise awareness about not sharing personal information. Additionally, enhancing cooperation between law enforcement agencies and judiciary at national and international levels, with a focus on protecting children and youth in the digital space.

Second Standard: Community Awareness:

Effectively countering cyber crimes and threats requires comprehensive awareness programs targeting citizens of various demographics, and the necessity of engaging civil society in these dynamics.

Third Standard: Strengthening Partnerships:

With governmental and private sectors, institutions, international organizations, and stakeholders.

Fourth Standard: Capacity Building:

Through the development and implementation of accredited training curricula by universities and accredited institutes, and enhancing capacities of various organizations in the fields of cyber security, electronic transactions, and digital transformation.

Fifth Standard: Dynamic Environment for Cyber Security:

Emphasizing scientific research and innovation in cyber security, network protection, and information systems, enhancing skills, and qualifying national competencies in information security and cyber crimes.

Sixth Standard: Development of Methods to Ensure Digital Security System, which should focus on three fundamental pillars:

- Prevention of cyber attacks and threats using firewall and security software against viruses, worms, and malware.
- Detection and recovery: Swift detection of threats and vulnerabilities and system updates.
- Rapid response: If attacks are detected and not countered in a timely manner, detection loses its value and importance. Therefore, readiness to respond, defend, and respond to various attacks is crucial.

Seventh Standard: Innovation and Investment:

Countering digital risks such as cyber crime, terrorism, and electronic attacks requires attracting and appropriately training human resources, enhancing innovation and investment, and achieving excellence in cyber security based on developing digital infrastructure that contributes to realizing Egypt's Vision 2030.

2. Proposed Model for Developing and Enhancing Digital Security and Information Safety to Combat Cyber Crimes and Attacks:

A- Approaches to Combat Cyber Crimes and Attacks include:

Governance - Community Awareness - Law Enforcement - International Cooperation - Training and Capacity Building - Support for Research, Development, and Innovation.

B- Partners in Combating Cyber Crimes and Attacks (Stakeholders):

Governmental Organizations - Private Sector - International Organizations - Academic Institutions.

C- Tools for Combating Cyber Crimes and Attacks:

Conferences - Seminars - Conventions - Committees - Workshops - Programs - Campaigns - Meetings - International Agreements.

D- Targeted Issues:

Cyber Crimes - Cyber Attacks - Malware - Cyber Terrorism - Cyber Warfare - Cyber Espionage - Cyber Sabotage - Artificial Intelligence - Internet of Things (IoT) - Social Engineering - Blockchain - Cyber Resilience - Quantum Computing - Biometric Hacking - Identity Theft - Device Hacking - Privacy Loss.

E- Targeted Groups:

At the individual level:

Children - University Students - Employees - Youth Victims of Cyber Crimes - Youth Victims of Cyber Attacks - Youth Perpetrators of Cyber Crimes.

At the national level:

- Countries with rising rates of cyber crimes.
- Countries experiencing cyber attacks.
- Countries affected by cyber terrorism.
- Countries affected by social engineering crimes.

F- Targeted Outputs aim to:

Establish best practices in digital, information, and cyber security and their security and technical controls.

- Reduce the impact of risks, attacks, and cyber crimes.
- Enhance capabilities to handle digital and security incidents.
- Build an organizational framework to protect current and emerging technologies.
- Detect cyber attacks and enhance incident recovery methods.

Eighth:

Study Results and Recommendations:

1. Results:

The study concluded several findings and recommendations that can be highlighted as follows:

1- There are several national and international definitions for the terms of cyber security, digital security, and cyber crimes. Concepts continuously evolve due to technological advancements, emerging technologies, and changes in communication systems and information technology. Establishing a comprehensive definition for digital security is challenging due to its novelty and the differing interpretations among researchers.

2- Digital security is an urgent necessity imposed by technological advancement and the digital transformation system to ensure the safety and security of information and communication technologies.

3- There is difficulty in categorizing types of electronic crimes and cyber attacks due to criminals' reliance on rapidly changing technologies and methods associated with technological advancements.

4- Study results showed that cyber attackers exploit known vulnerabilities in individuals, organizations, and countries, resulting in diminished capability to assess damages and increased risks. It is also challenging to accurately determine the direct and indirect costs incurred.

5- Results clarified that electronic crimes and cyber attacks significantly impact the social fabric of nations, as they are transcontinental crimes targeting infrastructure and social activities related to individuals and communities as a whole.

6- Electronic and cyber crimes pose a serious and increasing threat, with the costs of combating and detecting their effects being substantial for countries, given their complete reliance on modern and advanced technologies.

7- Cyber crimes and attacks undermine individuals' trust in governments due to their capability to cause immense harm. Governments are thus required to protect their citizens from a new generation of cyber attacks.

8- Findings indicated that most countries worldwide have experienced numerous cyber crimes and attacks targeting vital sectors of society. Consequently, they have enacted various laws to overcome the threats and dangers posed by them.

9- Results highlighted that Egypt is among the first countries to enact legislation, establish specialized centers and councils, and develop numerous strategic programs. Conferences have been held to protect the state from the risks of cyber crimes and attacks, aiming to create a safe and reliable digital environment for the diverse Egyptian society.

2. Proposals:

In light of the study's findings, the study suggests the following:

1- Addressing cyber crimes and threats requires enhancing knowledge and awareness among internet and social network users to avoid direct and indirect cyber incidents and damages that they might be exposed to or become victims of, thus reducing the costs incurred by the state in confronting them.

2- It is imperative to activate strategies, laws, and policies for digital security as they are essential means to achieve Egypt's national security, disseminate digital security culture among various societal groups, and integrate it into various regional and international plans and strategies to achieve cyber safety and information security in line with rapid changes.

3- Universities, institutes, and various organizations should focus on developing and teaching cyber security curriculum to make it a university requirement, ensuring the necessary scientific and technical expertise to combat advanced and evolving electronic attacks and threats.

4- Policy makers, academics, and specialists should consider the best ways to implement the concept of risk management associated with protecting privacy, data, and information from potential threats.

5- Building trust is essential in the digital environment and developing privacy protection strategies, addressing vulnerabilities and emerging new threats, and confronting security risks and privacy challenges. Attention must be given to ethical trust-building as it impacts the digital environment.

6- Decision makers should deal with digital security risks as a threat to political, economic, social, and technological security.

7- National strategies aimed at achieving digital security should reflect societal vision and enhance privacy protection in the digital space that relies on data as a fundamental cornerstone.

8- Digital security strategies should contribute to enhancing collaboration with stakeholders, benefiting from them, establishing best practices, and reaching possible solutions to manage risks in the digital space and enhance risk management practices.

9- Institutions and small startups should increase awareness among digital technology managers about privacy risks.

10- Enhancing awareness of digital citizenship among young people aged 18-40 on how to interact with the digital environment and various technology tools to achieve personal and societal benefits positively.

11- Raising awareness about safe use of electronic cards to enhance resilience against unauthorized uses in electronic transactions.

12- Issuing periodic newsletters on electronic crimes, cyber threats, and mechanisms to deal with them.

13- Training workers in various sectors, especially the information security sector, on developments and advancements in information and communication technology to minimize and combat cyber threats.

14- Efforts should be accelerated to activate legislation on artificial intelligence in line with Egypt's Vision 2030 and the National Cyber Security Strategy.

References:

(1) OECD Digital Economy Papers Managing Digital security and Privacy Risk, 2016 Ministerial Meeting on the Digital Economy, Back Growth Report the Digital Economy innovation, Growth and social prosperity, 2016, p, 5.

(2) Oced digital Economy papers ,Op cit p.5

(3) Bernat :Enhancing the digital security of critical activities, Going Digital Toolkit Note, 2021 No. 17. P.4.

(4) Op. Cit, P. 4.

(٥) ذياب البدانية : الجرائم الإلكترونية، المفهوم والأسباب، ورقة مقدمة فى الملتقى العلمى- الجرائم المستحدثة فى ظل التغيرات والتحولات الإقليمية والدولية ٢-٤/٩/٢٠١٤م عمان - الأردن.

(٦) فوزى حسين الزبيدى : منهجية تقييم مخاطر الأمن القومى : دراسة تحليلية لمنهجية تقييم مخاطر الأمن القومى NSRA، رؤى استراتيجية، مركز الإمارات للدراسات والبحوث الاستراتيجية، المجلد (٣) العدد (١١)، ٢٠١٥م، ص ١١ى.

(٧) أولريش بك، مجتمع المخاطر العالمى بحثًا عن الأمن المفقود، ترجمة علا عادل وآخرون، القاهرة، المركز القومى للترجمة، ٢٠١٣م، ص٢١٤.

(8) Jarvis, Darry I S "Theorizing Risk: Ulrich Beck, Globalization and Risk of the Risk society" Lee Kaun Yew School of public policy, National University of sing pore , p 3

(٩) نجـوان أحمد عاصم عبد الجـواد : الجريمة السيبرانية وتأثيرها على الأمن القومى المصرى، دراسة سوسيو تحليلية، جامعة الفيوم، مجلة كلية الآداب، الإنسانيات والعلوم الاجتماعية، المجلد (١٥)، العدد (١) يناير ٢٠٢٣م، ص ٢١٠٤.

(١٠) إسلام فوزى : الأمن السيبرانى، الأبعاد الاجتماعية والقانونية، تحليل سوسيولوجى، القاهرة، المجلة الاجتماعية القومية، المجلد السادس والخمسون، العدد الثانى، مايو ٢٠١٩م.

(١١) مكتب الأمم المتحدة المعنى بالمخدرات والجريمة : دراسة شاملة عن الجريمة السيبرانية، فيينا، ٢٠١٣م، ص ٧.

(12) Suhasini Verma, (et. al): Mounting Cases of Cyber- Attacks and Digital payment. India, 2023.P.61

(13) Yuchong Li, &, Qinghui Liu: A Comprehensive Review Study of Cyber- attacks and Cyber Security; Emerging trends and recent developments Energy reports,2021, P.8179.

(١٤) سامـى محمـد بونيـف : دور الاستراتيجيات الاستباقية فى مواجهـة الهجمات السيبرانية، الـردع السيبرانـى إنموذجًا.المجلة الجزائرية للحقوق والعلوم السياسية، المجلد (٤) العدد (٧)، ٢٠١٩م، ص ١٢

(15) Yuchong Li, & Qinghui, Liu, 2021 op. cit., P.8180

References:

(١٦) خورجى فلوريس كايبخاس، عائشة عفيفى، نيكولاى لوزنيسكى : الأمن السيبرانى فى مؤسسات منظومة الأمم المتحدة تقرير وحدة التفتيش المشتركة، الأمم المتحدة ، ٢٠٢١م، ص٧.

(١٧) أمنية عبيشات: الأمن الرقمى – قراءة فى مفهومه واستراتيجية حمايته، مجلة المسار للدراسات القانونية والسياسية، المجلد (١) العدد (١) ٢٠٢٣م، ص ١٠٠ .

(١٨) مركز هردو لدعم التعبير الرقمى: الأمن الرقمى وحماية المعلومات، الحق فى استخدام شبكات آمنة، القاهرة ،٢٠١٧ ، ص ٦

(١٩) أمينة عبيشات (٢٠٢٣م): مرجع سابق ، ص ٩٩.

(20) Sakshi Singh&Suresh Kumar: THE TIMES OF CYBER ATTACKS: ACTA TECHNICA CORVINIENSIS – Bulletin of Engineering TOME XIII 2020 FASCICULE 3, July – September, P 134-135

(٢١) نشرة تكنولوجيا المعلومات والاتصالات للتنمية فى المنطقة العربية – اللجنة الاقتصادية والاجتماعية لغربى آسيا (الإسكوا): الأمم المتحدة نيويورك، العدد (١٨) ٢٠١٢م، ص ١٠ .

(22) Digital Notes on cyber security, Department of information technology, Malla Reddy College of Engineering & Technology India ,2021, pp7-9

(٢٣) الاستراتيجية الوطنية للأمن السيبرانى (٢٠٢٣م –٢٠٢٧م)، وزارة الاتصالات وتكنولوجيا المعلومات.

(٢٤) خورخى فلوريس كايبخاس، عائشة عفيفى، نيكولاى لوزنيسكى ٢٠٢١م. مرجع سابق ، ص ١٤

(25) Lynn Batten, & Gang Li, : Application and Techniques in information security international conference Atis 6 th . Osaka University, Osaka, Japan.2016 P, 60

(٢٦) تقرير (TTU) الوثيقة RPM-ARB 1044- A قطاع تنمية الاتصالات، الاجتماع الإقليمى التحضيرى للمؤتمر العالمى لتنمية الاتصالات ٢٠١٠م لمنظمة الدول العربية، دمشق، الجمهورية العربية السورية، ١٧–١٩ يناير ٢٠١٠م.

(27) Nadiya Kostyuk, & yuri M. Zhukov: Invisible Digital front can cyber Attacks Shape Battlefield Events. Journal of Conflict Resolution, Vol 63 (2), 2019, P. 318.

(28) Hemraj, Saini, & Yerra shanker Rao, & T.C Panda: cyber- crimes and their Impacts, A review. International Journal of Engineering research and Application (IJERA) no/2. 2012, P 209

(29) Mario Spremié, & Alen Simunic,: Cyber Security Challenges in Digital Economy,2018. P 979.

(30) Proceedings of the world congress on Engineering No/ 1 London

(31) Mario Spremié, &, Alen, Simunic ,Op. cit., p 979

(32) Ryan Shandler, &, Miguel Alberto Gomez: The hidden threat of cyber- attacks- undermining public confidence in government, Journal of information technology & politics .2022 p 363

(٣٣) إسلام فوزى : مرجع سابق ، ص ١١٢ – ١١٣.

(34) James A. Lewis: Op Cit.

(٣٥) الاستراتيجية الوطنية للأمن السيبرانى (٢٠١٧م - ٢٠٢١م).

(36) https://mcit.gov.eg/Ar/Media_Center/Press_Room/Press_Releases/67460

تاريخ الدخول ٢٤/٤/ ٢٠٢٤م الساعة ١١,٥٠ مساء

(٣٧) الدستور المصرى ٢٠١٤م.

(٣٨) القانون رقم ١٧٥ لسنة ٢٠١٨م قانون مكافحة جرائم تنقية المعلومات.

(٣٩) القانون رقم ٩٤ لسنة ٢٠١٥م لمكافحة الإرهاب.

(٤٠) الاستراتيجية الوطنية للذكاء الاصطناعى، يوليو ٢٠٢١م . وزارة الاتصالات وتكنولوجيا المعلومات .

(٤١) الاستراتيجية الوطنية للأمن السيبرانى (٢٠١٧م – ٢٠٢١م) .

(٤٢) استراتيجية الحوسبة السحابية الحكومية ، ٢٠١٤ م ، وزارة الاتصالات وتكنولوجيا المعلومات .

(٤٣) الاستراتيجية الوطنية للأمن السيبرانى (٢٠٢٣م – ٢٠٢٧م) .

(٤٤) مصر والأمن السيبرانى : الهيئة العامة للاستعلامات https://www.sis.gov.eg/Story/258293 تاريخ الدخول ٢٥/٤/٢٠٢٤م الساعة ١١:٤٧ مساء

(٤٥) المرجع السابق

(٤٦) المرجع السابق

The social repercussions and risks of crimes and cyber-attacks on digital security and coping mechanisms in light of Egypt's Vision 2030

■ *Prof / Asmaa Jaber Mahran*
Assistant Professor of Sociology of Criminology
Faculty of Arts - Assiut University

Abstract:

The current study aimed to provide a sociological analysis of the social risks of crimes and cyber attacks on digital security and monitor the mechanisms and efforts of the Egyptian state in light of Vision 2030. The results showed that digital security is an urgent necessity imposed by technological development and the digital transformation system to ensure the safety and security of information and communications technology.

The results showed that most countries in the world were exposed to many crimes and cyber attacks that targeted vital sectors of society, and then issued various laws in order to overcome the threats and dangers resulting from them. The results showed that Egypt is one of the first countries to enact legislation and laws, establish specialized centers and councils, develop many strategies that include many different strategic programs, and hold conferences in order to protect the state from the dangers of crimes and cyber attacks, and to achieve a safe and reliable digital environment for Egyptian society with its various sectors.

Keywords: Cyber-crimes, cyber-attacks, digital security, Egypt Vision 2030

الانعكاسات والمخاطر الاجتماعية للجرائم والهجمات السيبرانية على الأمن الرقمى وآليات المواجهة فى ضوء رؤية مصر ٢٠٣٠

■ أ.م.د/ أسماء جابر مهران
أستاذ علم اجتماع الجريمة المساعد – كلية الآداب – جامعة أسيوط

المستخلص :

هدفت الدراسة الراهنة إلى تقديم تحليل سوسيولوجى للمخاطر الاجتماعية للجرائم والهجمات السيبرانية على الأمن الرقمى ورصد آليات وجهود الدولة المصرية فى ضوء رؤية مصر ٢٠٣٠ .

لقد أظهرت النتائج أن الأمن الرقمى يعد ضرورة ملحة فرضها التطور التكنولوجى ومنظومة التحول الرقمى لضمان سلامة وأمن المعلومات وتكنولوجيا الاتصالات .

بيَّنت النتائج أن معظم دول العالم تعرَّضت للعديد من الجرائم والهجمات السيبرانية التى استهدفت القطاعات الحيوية فى المجتمع، ومن ثم قامت بإصدار القوانين المختلفة من أجل التغلب على التهديدات والأخطار الناجمة عنها. أوضحت النتائج أن مصر من أوائل الدول التى قامت بسن التشريعات والقوانين وإنشاء المراكز والمجالس المتخصصة، ووضع الكثير من الاستراتيجيات التى تتضمن العديد من البرامج الاستراتيجية المختلفة، وعقد المؤتمرات من أجل حماية الدولة من مخاطر الجرائم والهجمات السيبرانية، ولتحقيق بيئة رقمية آمنة وموثوقة للمجتمع المصرى بمختلف أطيافه.

الكلمات المفتاحية : الجرائم السيبرانية، الهجمات السيبرانية، الأمن الرقمى، رؤية مصر ٢٠٣٠