SCIENTIFIC CULTURE

www.sci-cult.com

*SCIENTIFIC CULTURE, Vol. 11, No. 3.2, (2025), pp. 1610-1626*
*Open Access. Online & Print*

**DOI: 10.5281/zenodo. 19439836**

# THE CONTRIBUTIONS OF THE SAUDI CYBERSECURITY AUTHORITY TO REDUCING THE RISKS OF CYBERCRIME

**Dr. JAFAR MOHAMMED IBNSHAFLOOT**

*Associate Professor of Criminology , Naif Arab University for Security Sciences, Saudia Arabia*

**Received: 27/10/2025**
**Accepted: 27/11/2025**

*Corresponding Author:*

**Abstract**:
The rapid advancement in information and communication technologies has led to their deep integration into various aspects of daily life, becoming a fundamental basis for interactions among individuals, companies, and institutions. Moreover, electronic information networks have increasingly been adopted as a global means of communication across all fields. While this technological expansion has contributed to saving time, effort, and distance, it has also resulted in numerous risks, the most significant and impactful of which is cybercrime.These crimes have emerged primarily from the unlawful use of data and information stored in computers and digital systems, leading to a noticeable increase in transnational and cross-border crimes. This escalation is closely associated with the widespread reliance on modern technologies—such as computers and smart devices—in education, social communication, and the completion of governmental services. Consequently, digital data have become highly vulnerable to hacking and unauthorized access, posing serious threats to individuals, institutions, and states.In response to these challenges, the field of information security has emerged as one of the most critical sciences of the modern era, with cybersecurity becoming an essential component of national security. The Kingdom of Saudi Arabia is considered one of the leading countries that have prioritized cybersecurity, recognizing the growing dangers posed by organized cybercrimes that exploit the open cyberspace. Such crimes represent severe threats to state stability and security, not only through economic losses but also through the theft of sensitive and strategic information.

**Keywords:** (Cybersecurity – Risks – Contributions – Cybercrime)

## INTRODUCTION:

The Problem Statement of the Study: Digitalization in the modern era has become a fundamental pillar of advanced societies, significantly impacting various aspects of daily life, including the economy, education, and health—indeed, all facets of life. This has prompted countries to focus on the rapid developments in the information and communication technology sector. (Al-Anzi, 2020(

Despite the positive effects of digitalization, its negative impacts have affected individuals, institutions, and nations. Perhaps the most serious of these are cybercrimes, which threaten the security and safety of all countries, as they are a global phenomenon not limited to any one nation, even though they may vary in their forms.

The Kingdom of Saudi Arabia is among the first countries to prioritize cybersecurity as a result of the information revolution and the tremendous development in modern communication technologies. This has led to a variety of cybercrimes, including electronic fraud, electronic forgery, privacy violations, and electronic financial transactions. Numerous studies have emphasized the necessity of enacting legislation and laws to curb these crimes. (Al-Shahri, 2019) The reality of cybercrime in the Kingdom of Saudi Arabia can be identified, along with future challenges, confirming that cybercrime is a negative consequence of technology and is on the rise (Al-Amin, 2013). Therefore, it is necessary to enact legislation and implement measures to curb cybercrime, develop monitoring systems, and provide specialized cybersecurity training for employees. Furthermore, documenting cybercrime and studying the objective aspects of its elements is crucial. The study concluded by emphasizing the need to establish a national authority specializing in cybercrimes (Rawan, 2020). Cybercrime, its characteristics, elements, and motives can also be clarified. Additionally, the Saudi regulator must establish a system for digital procedural measures to keep pace with the digital transformation the Kingdom is undergoing (Al-Otaibi Arian, 2021.(

An analysis of cybercrime and its anti-crime law reveals that cybercrimes are on the rise throughout the Kingdom, and protecting against cyber threats represents an ongoing administrative challenge for state institutions. (Elnaim B. E. December 2013(

One of the most important factors in achieving national cybersecurity is the use of the latest technological protection systems. The study also emphasized the need to raise awareness of the importance of cybersecurity. (Al-Anzi, Majid bin Khalaf Hamoud 2020(

The reality of cybercrime within the Kingdom of Saudi Arabia confirms that the negative exploitation of technology has given rise to a set of concepts, including what is known as cybercrime and its extreme danger to societies (Bushra Al-Amin 2013.(

The study seeks to address the lack of regulation in the Saudi cyberspace. Most crimes are committed with the aim of generating profits and achieving financial gains, and there is a particular security challenge for crimes committed from abroad.

)Elnaim B. E. December 2013) Therefore, the current challenge for the state is to confront transnational cybercrime and create mechanisms to aid in the investigation and legal prosecution of cybercriminals (Khaled, Nada Al-Damras, 2019). This study aligns with other studies that aimed to identify the characteristics of these crimes. For example, Al-Maqsoudi's 2017 study indicated that rapid changes in cyberspace have led to an increase in the rate of cybercrime, necessitating international cooperation to curb its spread.

Additionally, Al-Alwan's 2023 study concluded that there are interdependent and interconnected relationships between each stage, and that each stage faces rapid challenges due to the swift changes in cyberspace.

Al-Shahri's 2019 study emphasized the necessity of addressing cybercrime through legislation and regulations.

Furthermore, Al-Maqsoudi's 2017 study highlighted differences in technical and technological aspects and stressed the need for international cooperation to limit its spread.

This study also agreed with the findings of Abdul-Razzaq (2021), which concluded that artificial intelligence has contributed to an increase in cybercrimes and emphasized the need for international cooperation to combat them.

It also agreed with the study by Al-Khatib (2019), titled "Cybercrimes via Social Media," which emphasized the necessity of establishing specialized agencies to combat all crimes committed on social media platforms.

The study by Al-Haif and Al-Anzi (2018), titled "Cybercrimes: Types and Dangers," revealed the importance of preventing cybercrimes by intensifying awareness campaigns through media outlets and providing protection programs.

The study by Nmreze, Alerhanianl, and Humaun (2021) concluded that all students who were victims of cybercrimes were unaware of local laws and regulations in the Kingdom of Saudi Arabia. Therefore, the study recommended highlighting, strengthening, and disseminating these laws, as well as increasing

awareness programs about internet crimes and how to deal with them according to local legislation. A study by Ganesh S.SET. All (2020) confirmed that individuals working in the technology sector are more knowledgeable about cybercrime than the general public.
A study by Kumar and Soman (2018) revealed the security risks of social media, cyber threats and dangers, and techniques for preventing and mitigating them.
Therefore, the question that seeks an answer is: How does the Anti-Cybercrime Authority contribute to reducing cybercrime, and what are the most frequently addressed issues?
Based on the theoretical literature presented in this study, the current research focuses on the following questions: What are the contributions of the Anti-Cybercrime Authority in Saudi Arabia to reducing cybercrime? The main question is: "What are the contributions of the Anti-Cybercrime Authority in Saudi Arabia to reducing cybercrime?"

**This main question branches into several sub-questions:**
1- What programs are offered to individuals and government entities to reduce cybercrime?
2- What are the most important recommendations from previous studies for reducing cybercrime? 3- What findings does this study offer that contribute to reducing cybercrime?

**Study Significance:**
**First: Theoretical Significance of the Study**
1. This study contributes to directing the attention of researchers in the field of social work and social sciences in general to the importance of cybersecurity as a contemporary societal issue related to protecting individuals and institutions from the risks of cybercrime.
2. The study gains its theoretical significance by shedding light on one of the cybersecurity programs in the Kingdom of Saudi Arabia, reflecting the Kingdom's keeping pace with the rapid transformations in the use of information and communication technology.
3. The study represents a new scientific addition to the Saudi and Arab libraries, given its focus on analyzing the contributions of cybersecurity programs within the Kingdom to combating cybercrime from a social perspective.
4. The theoretical significance of the study stems from the continuous increase in the number of internet users at both the local and international levels, and the accompanying growth in social risks associated with the unsafe use of digital technologies.

**Second: The Applied (Practical) Significance of the Study**
1. The study's practical significance lies in its focus on a vital program currently in place to combat cybercrime, in light of the Kingdom of Saudi Arabia's Vision 2030, which aims to achieve digital transformation and enhance cybersecurity.
2. The study's findings may contribute to providing cybersecurity professionals in the Kingdom with a future-oriented perspective that will help develop and improve the "Hosni" program to meet emerging challenges.
3. The study's practical significance is highlighted by demonstrating the benefits and positive impacts achieved through the program's implementation, thus supporting national efforts to achieve cybersecurity as a requirement of social security.
4. The study provides a scientific analysis of the methods and mechanisms of the cybersecurity system in addressing cybercrime, which can be used to develop preventive and remedial policies and programs.
5. The study may yield a set of practical recommendations that contribute to enhancing the effectiveness of the "Hosni" program and support its role in mitigating the risks of cybercrime and protecting society. Research Objectives:

**This study aims to achieve a set of measurable objectives, which are as follows:**
1. To determine the extent of the Saudi National Cybersecurity Authority's contributions to mitigating the risks of cybercrime, through an analysis of the regulatory, legislative, and awareness frameworks adopted by the Authority.
2. To assess the level of awareness among target groups (youth, families, and educational institutions) regarding cybercrime and methods of prevention, in light of the programs and initiatives offered by the National Cybersecurity Authority.
3. To identify the most significant social and professional obstacles that hinder the optimal utilization of the National Cybersecurity Authority's efforts in combating cybercrime, from a social work perspective.
4. To evaluate the role of social work in building digital values and ethics among individuals, thereby contributing to reducing engagement in risky online behaviors.
5. To develop a proposed social work-based approach to enhance the integration of security and social efforts in combating cybercrime, based on the study's findings. Research Procedural Concepts:

**First: Cybercrime:**

**Definition of Cybercrime:**

Cybercrime is defined as any illegal behavior, act, or practice committed through the use of digital devices or modern technologies, with the aim of achieving material or non-material gains through unlawful means, such as theft, hacking, data breaches, and the misuse of information in a way that harms individuals or institutions.

**Concept of Cybercrime:**

Cybercrime refers to a set of acts related to technical and technological aspects, which may be characterized by their novelty and continuous development. Its commission relies on the use of computer technologies and information systems, and requires specialized technical expertise, both in its execution and in the procedures for investigating and prosecuting its perpetrators (Sabaya, 2022, pp. 37–38).

Cybercrime is also considered any type of crime stipulated in the Penal Code, whenever its commission is linked to the use of information technologies or digital communication methods (Al-Junaidi, 2022, p. 63).

Cybercrime is also considered any type of crime stipulated in the Penal Code, whenever its commission is linked to the use of information technologies or digital communication means (Al-Junaidi, 2022, p. 63).

Munir and Shabir G (2018) defined cybercrime as any illegal activity carried out using computers, digital devices, and internet-connected networks, facilitated through an internet intermediary. This may include the remote theft of information belonging to individuals or institutions through unauthorized access to electronic systems.

Operational Definition of Cybercrime: (Al-Khabiri, Badr, 2022).

**In this study, cybercrime can be operationally defined as:**

- An act that contradicts sound social conduct.
- Any behavior that violates the provisions of the law.
- Requires knowledge of computer technologies and information systems.
- Is committed physically through the internet or digital media.
- Entails legal accountability and effective prosecution according to applicable legislation.

**Second: Cybersecurity:**

Cybersecurity is defined as the protection of networks, information systems, data, information, and internet-connected devices. This includes a set of preventive procedures, measures, and standards aimed at reducing the risks of cyberattacks and minimizing their negative impacts (Jabour, 2017).

Cybersecurity is also viewed as the process of organizing and integrating resources, procedures, and systems to prevent or reduce various forms of cyberattacks, which are carried out illegally in cyberspace.

**Third: The Anti-Cybercrime Law:**

The Anti-Cybercrime Law in the Kingdom of Saudi Arabia was established by Royal Decree No. (17) dated 8/3/1428 AH. Article 1 of the law, specifically clause (8), stipulates that a cybercrime is any act committed using a computer or information network in violation of the provisions of this law. Article 2 of the law affirms that its primary objective is to reduce the occurrence of cybercrimes by defining the types of these crimes and specifying the penalties prescribed for each. Article 3 clarifies that anyone who commits any of the following cybercrimes, such as eavesdropping on communications transmitted over information networks, threatening and blackmailing individuals, unauthorized access to websites with the intent to alter, damage, or modify them, violating privacy through the use of mobile phones, or defaming others, shall be punished by imprisonment for a period not exceeding one year, or by a fine not exceeding five hundred thousand riyals, or by one of these two penalties.

## THEORETICAL GUIDELINES FOR THE STUDY:

**Giddens' Risk Theory (Globalization and Risk):**

- This theory indicates that we live in a world where we are threatened by man-made dangers to the same degree as, or even more than, external dangers.
- Furthermore, technological changes at the local and global levels will have serious consequences.

He argues that risks are divided into external risks, which originate from nature, such as floods, famines, and epidemics.

And artificial risks, which are those resulting from globalization and are caused by human activity that alters nature, or risks arising from technological and intellectual advancements.

**Accordingly, the theory's tactics in this study can be identified as follows:**

1- Individuals with repressed criminal behavior in the physical world are more inclined to commit crimes in cyberspace, crimes they would not otherwise commit in the physical world due to their circumstances and location.

2- The flexibility of identity, the anonymity of perpetrators, and the lack of deterrents in

cyberspace facilitate the commission of cybercrimes.
3- It is possible for criminal behavior in cyberspace to be imported into the physical world, and vice versa.
4- Cyberspace offers opportunities for criminals to engage in sporadic activities.
5- In cyberspace, strangers may collaborate to commit crimes in the physical world.
6- It is possible for partners in the physical world to collaborate to commit cybercrimes. 7. Individuals in closed societies are more prone to committing cybercrimes.
8. The values and rules of the physical world may conflict with the standards and values of cyberspace.

**Theoretical Framework of the Research:**
**Characteristics of Cybercrimes:**
There are several definitions of cybercrime, including: Cybercrime is defined as any criminal activity committed using the internet.
It is a criminal phenomenon that society has recently been suffering from, involving violations of electronic rights and privacy. Computers in general, and the internet in particular, have become tools for committing cybercrimes (Ben Amer, 2021, p. 803).
It has also been defined as an illegal activity aimed at copying, accessing, altering, or accessing information stored on a computer (Amara, 2019, p. 82).
The Saudi Anti-Cybercrime Law stipulates in Article 1 that a cybercrime is any act committed using a computer or information network in violation of the provisions of this law (Text of the Anti-Cybercrime Law, 2007).

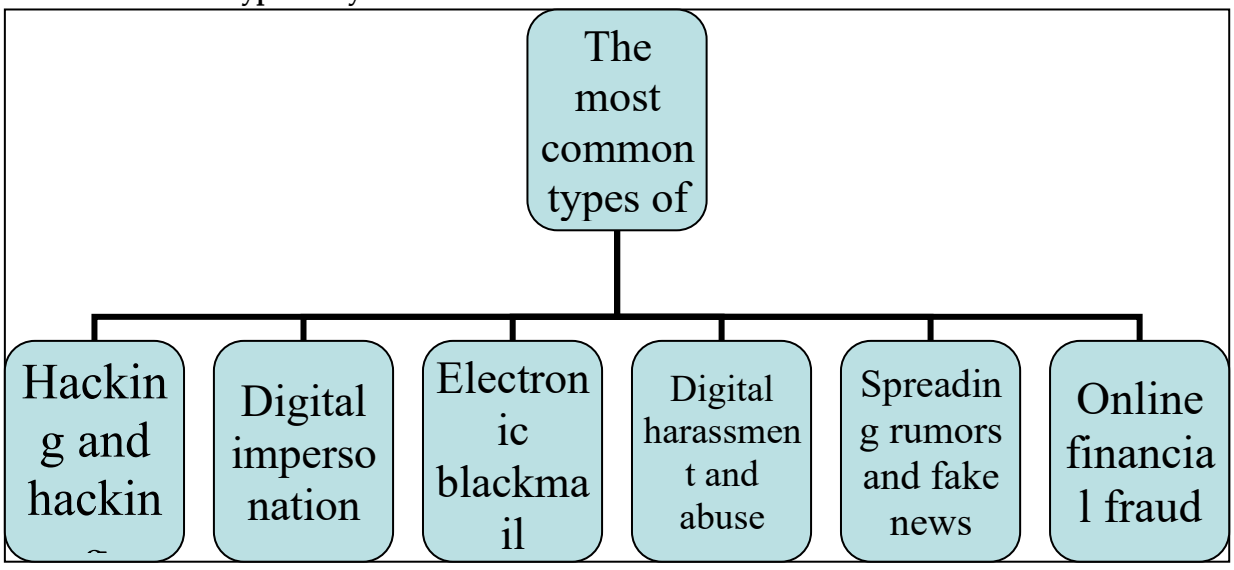
**It is also defined as a criminal act that uses a computer as the primary tool in its commission.**

**Cybercrimes are characterized by a number of features, including:**
(a) They rely on new technologies such as computers and the internet to commit the crime.
(b) They are not limited by geographical boundaries; rather, they are transcontinental.
(c) The perpetrators are difficult to prosecute because they use fake identities and pseudonyms.
(d) They are easy to commit, unlike traditional crimes.
(e) They are quick to commit. Cybercrimes, as classified by Chawki, include:
A- Economic Computer Crimes, which include information theft, cyber espionage in the business sector, computer software hacking, data destruction, crimes related to using computers to conceal manipulation by managers of financial institutions, crimes related to violating privacy, and crimes that threaten national interests or the personal safety of individuals.

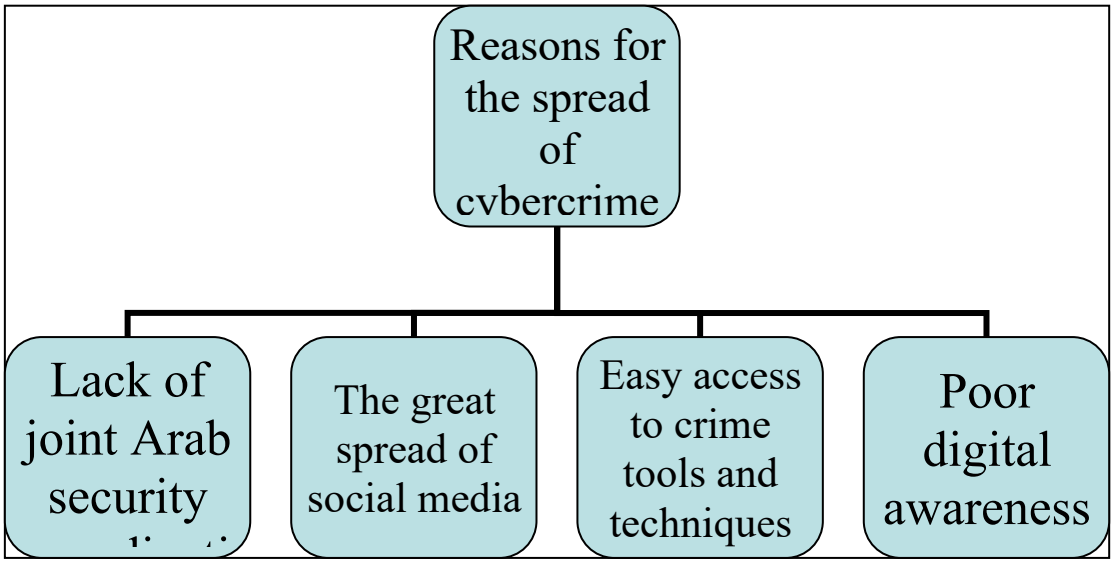
**Some of the most prominent types of cybercrimes include:**
- Publishing information.
- Hacking.
- Selling malware on devices or data.
- Collecting and storing personal data illegally.
- Impersonating someone or using their identity for illegal purposes.
- Cyber extortion.
- Cyber defamation.
- Cyber theft.
- Cyber harassment.
- Cyber espionage.

- Manipulating, disabling, or altering the data of systems.

**The most common types of cybercrimes**



**Reasons for the spread of cybercrime**




The effects of cybercrimes include: psychological harm to victims, direct and indirect financial losses, damage to personal or professional reputation, violation of privacy, and disruption of national security.

- The definition of cybercrime according to the Saudi system is any act committed using a computer or information network in violation of the provisions of this system.

1- The Anti-Cybercrime Law issued by Royal Decree No. M/17 dated 8/3/1428 AH.
The "Kulluna Amn" (We Are All Security) application: This application allows citizens and residents to submit security and criminal reports, reports related to violations of privacy, threats and blackmail, hacking of social media accounts, and other cybercrimes.

The "Bashar Bsad" (Humanity) application: There is no specific and updated number of reports, but figures are published periodically in news reports. In the first 45 days after the platform's launch, it received 28,000 reports, and this number exceeded 1.5 million by November 2018.

Methodological procedures of the study:
Type of study:
This is a descriptive and analytical study to describe the phenomenon under study in its various dimensions in order to reach results that contribute to understanding the contributions of the Anti-Cybercrime Authority.

**METHODOLOGY**:
The researcher used the descriptive-analytical method to describe the phenomenon under study in its various dimensions, aiming to arrive at conclusions that contribute to understanding the contributions of the Cybercrime Authority.

**RESEARCH TOOLS:**
The researcher relied on diverse tools that align with the nature and type of the methodological strategy used to achieve the study's objectives:
1- Interview Guide: Interviews with experts in the security field regarding the contributions of security personnel in reducing cybercrime and how to deal with it.
2- Content Analysis Guide: Studies conducted in Saudi society on cybercrime.
Steps Followed by the Researcher to Prepare the Interview Guide:
Regarding the Interview Guide: Procedures for Designing the Interview Guide: The researcher analyzed the theoretical literature and previous studies related to the study topic. Based on this analysis, the guide's themes and items were prepared. The first theme consisted of primary data, and the second theme focused on identifying the contributions of the Cybercrime Authority in reducing cybercrime. - Interview Guide Review Phase: Validity and Reliability
The initial draft of the guide was presented to eight expert reviewers who were asked to provide their opinions on the consistency of the guide's content with its intended purpose.
Based on the review results, statements that did not achieve an 80% rating were excluded, and some statements were added.

**Statistical Methods Used in the Study**
The statistical methods appropriate to this study were used, namely percentages, weighted frequencies, and percentages.

The face validity of the content analysis guide was assessed by presenting it to eight professors of criminology and social work. A rating of at least 80% was adopted, and the final version of the content guide was constructed. Instrument Reliability: The instrument's reliability was calculated by analyzing the content of five studies conducted on cybercrime in Saudi society. Psychoanalysis of these studies was performed at two-week intervals, and the results showed a reliability coefficient of 78%.

**Study Scope:**
Study Sample: This consisted of a comprehensive survey of published field studies related to cybercrime conducted in the Kingdom of Saudi Arabia.

- Available statistics on the prevalence of these crimes were also utilized.
- An interview guide for experts in the security field was reviewed by eight professors of criminology and social work. At least 80% of the review was conducted, and the final version of the interview guide was developed.

**Data Collection Tools:**
1- Examination of documents, research papers, studies, and scientific books in Arabic and English, as well as the 2023 Global Risks Report issued by the World Economic Forum.
2- Available statistics on cybercrime between 2022 and 2024.
3- Interview Guide for Public Security Personnel.

Table No. (1) Shows the sample of studies consulted.

| The year | the study | M |
|---|---|---|
| **2019** | **Study (Mohamed Massad,). A strategic vision for combating cybercrime, which is dear to human security. The study concluded that it is necessary to establish a specialized prosecution office** | **1** |
| **2019** | **Study (Ali Al-Shehri,). A strategic vision to reduce cybercrime to enhance cybersecurity in the Kingdom of Saudi Arabia. The study stressed the necessity of establishing more specialized courts, developing current technologies, and developing human cadres working in the areas of combating.** | **2** |
| **2018** | **Study by Abdul-Ilah Al-Mutairi, 2018). The role of the media in raising awareness of cybercrimes.** | **3** |
| | **A study by Rana Misbah Abdel Mohsen on mechanisms to combat cybercrime in the Kingdom of Saudi Arabia** | **4** |
| **2024** | **Study (Sumaya Musharraf Abdullah Al-Omari,). About cybersecurity and its role in raising the level of public security of the state - the Kingdom of Saudi Arabia as an example.** | **5** |
| **2020** | **A study (Alghamdi), which aimed to identify the nature and types of cybercrime in the Kingdom of Saudi Arabia and the role of combating cybercrime in enhancing cybersecurity. The study recommended the necessity of educating the Saudi community about ways to protect against cybercrime.** | **6** |
| **2020** | **Study (Al-Mutawa,). Titled: The level of awareness among students of the College of Education, Shaqra University, the system for combating information crimes** | **7** |
| **2018** | **Study (Al-Anazi, Al-Haith,). Information crimes, their types and seriousness.** | **8** |
| 2023 | **Study by (Abdo Suleiman Al-Rashidi, Abdullah Muhammad Al-Mahdawi,). The level of awareness of the system for combating information crimes among university students** | **9** |
| | **Sherihan Mamdouh Hassan's study of information crimes and ways to confront them at the national and international levels.** | **10** |
| 2023 | **.Study (Hamoud Nawar Al-Nimr), digital media and the crime industry, Saudi society** | **11** |
| 2020 | **Study (Al-Subaili, Sultan, Abdul Rahman Al-Shamer,) The role of digital media in reducing cybercrimes in the Kingdom of Saudi Arabia** | **12** |
| 2023 | **Study (Salma Saleh), the efforts of organizations to combat information crime in achieving cybersecurity.** | **13** |
| 2022 | **Study (Abdul Rahman, Shahd, Al-Raifi, Reem Ali,). The extent of graduate students' awareness of the system for combating information crimes in light of the digital transformation within the Kingdom's vision.** | **14** |

| | | |
|---|---|---|
| 2023 | **Study (Awatef Al-Qahtani), a proposed strategy for educating women about the system of combating cybercrimes.** | **15** |
| 2019 | **Study (Bandar bin Manahi Al-Qahtani,) The use of social networking sites in shaping the mental image of the citizen regarding electronic commerce crimes** | **16** |
| 2021 | **Study (Omar bin Muhammad Al-Namlah), information crimes and their social impact on individuals in Saudi society.** | **17** |

Table No. (2)
Shows the study sample according to job rank (n=20)

| Repetition | Ratio | Repetition | Age |
|---|---|---|---|
| **3** | **%10** | **2** | **lieutenant** |
| **Repeat 2** | **%6.6** | **3** | **Provided** |
| **1** | **%16** | **12** | **pioneer** |
| **Repeat 2** | **%6.6** | **3** | **Colonel** |

Colonel 3 6.6% 2 repeated

The table above shows the distribution of the military rank variable. The highest percentage is shown to be Major (16%), followed equally by Brigadier General and Lieutenant Colonel (6.6%). Lieutenant came in last (10%).

Table No. (3)
Shows age (n=20)

| Ratio | number | Age |
|---|---|---|
| **%50** | **10** | **less than 40 years old −30** |
| **%25** | **5** | **From 40 to less than 50 years old** |
| **%25** | **5** | **years and over 50** |

Table No. (4)
Shows the length of service (n=20)

| Ratio | number | Age |
|---|---|---|
| **%50** | **10** | **years old 13** |
| **%25** | **5** | **years old 25** |
| **%25** | **5** | **years old 32** |

Table No. (5)Illustrating the types of crimes handled by the Cybercrime Authority in the Kingdom of Saudi Arabia
(n=20)

| Rank | Its type | The crime | M |
|---|---|---|---|
| **1** | **Publishing private information** | **blackmail and threats** | **1** |
| **2** | **Impersonation** | **Cyber fraud** | **2** |
| **4** | **Data destruction or theft** | **Hacking or unauthorized access** | **3** |
| **3** | **Publishing private information** | **defamation** | **4** |
| **5** | **Data destruction or theft** | **Spreading Malicious Software** | **5** |
| **6** | **Data destruction or theft** | **Cyber espionage** | **6** |

Table No. (6)Illustrating the types of cyber threats faced by the Kingdom of Saudi Arabia
(n = 20)

| ratio | phrase | M |
|---|---|---|
| %59 | threat | 1 |
| %19 | Malware | 2 |
| %10 | threatening messages | 3 |
| %2 | Unauthorized access attempts | 4 |
| %2 | Eavesdropping and cutting off communications | 5 |

Table No. (7)Illustrating the sectors targeted by cyber threats
(n = 20)

| ratio | sector | M |
|---|---|---|
| %65 | government sector | 1 |
| %8 | Energy sector | 2 |
| %7 | Telecommunications sector | 3 |
| %3.4 | Technology, Resources & Utilities Sector | 4 |
| %2 | Health and financial services sector | 5 |
| %5 | Other sectors | 6 |

Table No. (8)
Shows the number of attacks dealt with by the Cybercrime Authority in the Kingdom of Saudi Arabia

| Year | Number of attacks |
|---|---|
| 2020 | 2244 |
| 2021 | 300.000 |

Source: Government Data, Saudi Data Authority Website 2023
Table No. (9)
Shows the number of cybercrime cases

| The accused | number | Year |
|---|---|---|
| 2713 | issue 2723 | 2021 |
| 5439 | issue 4783 | 2022 |

Source: Saudi Ministry of Justice

The rate of cybercrimes in 2022 increased by 55% in cases compared to 2021, and by 67% in the number of defendants for the same year.

Table No. (10) Illustrates the nature of the crimes dealt with by the Cybercrime Authority

| Order | ratio | The crime |
|---|---|---|
| 1 | %80 | blackmail and threats |
| 2 | %100 | Electronic fraud |
| 3 | %70 | Hacking and unauthorized access |
| 5 | %50 | Defamation and slander |
| 4 | %60 | Spreading Malicious Software |
| repeated 2 | %70 | Electronic espionage |

Table No. (11) Illustrates the obstacles that limit the contribution to reducing cybercrime

| repetition | % | Distance |
|---|---|---|
| 1 | %100 | The rapid diversification of crime patterns |
| 2 | %70 | Insufficient control over it |
| 3 | %60 | Fear of reporting among some citizens |
| 5 | %20 | legislation |
| 4 | %30 | Lack of international agreements with all countries |
| 6 | %10 | Lack of training courses for national talents |

Table No. (12) Explains the reasons for the spread of cybercrimes

| Order | ratio | number | Distance | M |
|---|---|---|---|---|
| 1 | %30 | 30 | Lack of digital awareness | 1 |
| 2 | %20 | 20 | Fraudulent calls and fake messages | 2 |
| 3 | %10 | 10 | Hacking major institutions | 3 |
| 3 repeated | %10 | 10 | Hacking major institutions | 4 |
| 2 repeated | %20 | 20 | The need for some laws | 5 |
| 3 repeated | %10 | 10 | High income from those crimes | 6 |

Table No. (13) Explains the reasons for the spread of cybercrimes

| Order | ratio | Distance | M |
|---|---|---|---|
| 2 | %50 | Electronic reporting via the national platform | 1 |
| repeated 2 | %50 | Kulna Amn app | 2 |
| 1 | %100 | Human Coordinator | 3 |
| repeated 2 | %50 | Official security guidelines | 4 |

Table No. (14) Illustrates the methods used for cybercrimes

| Order | ratio | Distance | M |
|---|---|---|---|
| ٤ | ٢٠ | Collecting and encrypting sensitive data | 1 |
| ٣ | ٣٠ | Unauthorized access to networks | 2 |
| ٣ | ٣٠ | Spreading viruses and malware | 3 |
| ٥ | ١٠ | fraudulent emails | 4 |
| ٣ | ٣٠ | Breach of security regulations | 5 |
| ٥ | ١٠ | Espionage and data theft | 6 |
| ١ | ٥٠ | extortion of individuals | 7 |
| ٢ | ٤٠ | Spreading fabricated information | 8 |

Table No. (15) Explains the reasons for the spread of cybercrimes

| Order | ratio | Distance | M |
|---|---|---|---|
| ٢ | ٢٠ | Lack of awareness among some members of society | 1 |

| | | | |
|---|---|---|---|
| ٣ | ١٠ | **The media's role is still insufficient to raise awareness of the dangers of these crimes.** | **2** |
| ١ | ٥٠ | **Increase in technology users** | **3** |
| ٢ | ٢٠ | **The absence of an international cooperation policy to prosecute the perpetrators of these crimes** | **4** |

Cybercrime Cases:
2723-2021
4783-2022
Defendants: 2713-2021
5439-2022
Source: Saudi Ministry of Justice (2022)
Cybercrime Case Statistics:
- Improving monitoring mechanisms.
- Increasing spending on cybersecurity.
- Building national capabilities.
- Raising community awareness.
- Expanding cybersecurity awareness and training programs.
- Developing legislation to keep pace with the evolution of cybersecurity.

Conducting further interdisciplinary studies between the fields of sociology and cybersecurity.

Table No. (16) Illustrating the types of cybercrimes that the Kingdom experienced from (2017 to 2023)

| Order | Year | Number | Types | M |
|---|---|---|---|---|
| ١ | **2023** | **2.3000000** | **cyber attacks** | **1** |
| ٢ | **2021** | **300.000** | cyber attacks | **2** |
| ٣ | **2020** | **daily 2244** | cyber attacks | **3** |
| ٤ | **2018** | **daily 150** | cyber attacks | **4** |

Table No. (17) Shows the number of cases

| Order | Year | Number | Types | M |
|---|---|---|---|---|
| ٢ | **2020** | **2723** | **Information issues** | **1** |
| | **2021** | | | **2** |
| ١ | **2022** | **4783** | | **3** |

Table No. (18)Illustrating the types of crimes that were dealt with legally

Table No. (19)Sectors targeted by cyber threats

| Order | ratio | Types | M |
|---|---|---|---|
| **1** | **%65** | **Government** | **1** |
| **2** | **%8** | Energy | **2** |
| **3** | **%7** | **Communications** | **3** |
| **5** | **%3.4** | **Technology, resources and benefits** | **4** |
| **6** | **%2** | **Health and financial services** | **5** |
| **4** | **%5** | **Unspecified sectors** | **6** |

Table No. (20) Types of Threats

| ratio | Types | M |
|---|---|---|
| **%59** | **threats** | **1** |
| **%19** | **Malware** | **2** |
| **%10** | **threatening messages** | **3** |
| **%2** | **Unauthorized entry** | **4** |
| **%2** | **Eavesdropping and the communications sector** | **5** |

Table No. (21) Explains the obstacles

| Order | ratio | Distance | M |
|---|---|---|---|
| ٢ | 30 | Lack of educational mechanisms for dealing with cybercrimes | 1 |
| ٤ | 10 | The lack of awareness programs that match its seriousness | 2 |
| ٣ | 20 | Some people don't know how to report | 3 |
| ٢ | 30 | Fear of reporting for fear of being dragged into it | 4 |
| ٣ | 20 | Lack of parental supervision over children's communication devices | 5 |
| ١ | 50 | The inability to identify the perpetrators of transnational crimes | 6 |
| ٤ | 10 | Lack of training courses in the latest developments in combating cybercrime | 7 |

Table No. (22) Explains the proposals

| Order | ratio | Distance | M |
|---|---|---|---|
| ١ | %50 | Securing vital networks | 1 |
| ٣ | %20 | Developing international security plans through international cooperation | 2 |
| ٢ | %40 | Using AI-based cybersecurity systems | 3 |
| ١ | %50 | Accurate tracking of cloud applications | 4 |
| ٢ | %40 | Raising awareness among citizens about the optimal use of digital platforms | 5 |
| ١ | %50 | Intensify awareness campaigns | 6 |

**Presentation and Interpretation of Study Results:**

Based on an analysis of the content of academic papers, available statistics and data on dealing with cybercrimes, as well as interviews with security personnel working in the information security sector:

- Previous studies have confirmed that technology is used in all types of cybercrimes, and criminals exploit artificial intelligence tools to commit these crimes. This technology is considered a source of new criminal and security threats.
- Despite the importance of technological development, it is a double-edged sword. While it has facilitated the rapid detection, containment, and prevention of crimes, it has also contributed to the spread of transnational crimes.
- Al-Alwan's 2023 study emphasized the existence of complex, evolving, and rapidly changing relationships that necessitate building human capacity with continuous awareness of developments in all branches of cyberspace. Al-Maqsoudi's 2017 study focused on the absence of an international law prohibiting and criminalizing cybercrimes. It explained that these crimes may be planned in one country and executed in another, highlighting the difficulty of prosecution. Al-Shahri's study concluded that combating cybercrime is the most significant threat facing the Kingdom of Saudi Arabia. These findings are determined in light of previous studies:

**Previous studies conducted in Saudi society on cybercrime have emphasized the necessity of:**

1- Developing a clear and comprehensive information security strategy across all sectors.
2- Encouraging the efforts of researchers in the field of information security, focusing on matters related to national interests and capacity building.
3- Organizing conferences and seminars that keep pace with developments, prepare for risks, and manage them effectively.
4- Employing the latest security technologies and equipment necessary for detecting and addressing risks.
5- Continuing to develop human resources working in the fields of combating cybercrime and cybersecurity.
6- Establishing specialized units, such as cyber police, to mitigate the risks of these crimes.
7- The establishment of a national authority for the prevention of cybercrime has contributed to reducing the number of such cases.

8- International cooperation is essential to combat these crimes and reduce their severity.

**In conclusion,** the current study differs from previous studies in several key aspects, most notably the methodology used, the methods employed, the type of study, the sample, the study population, and the emphasis placed on the contributions of the Anti-Cybercrime Authority in the Kingdom. In addition to analyzing previous studies in the field of cybercrime:
1- The diverse disciplines that addressed these studies, including social, legal, and media fields, each approaching the topic from its respective area of expertise, all agreed on the seriousness of these crimes and the necessity of raising awareness to reduce their occurrence.
2- The studies confirmed that citizens are aware of the dangers of cybercrime, and this responsible awareness has led to a decrease in certain forms, such as fraud and threats.
3- Legal studies emphasized the need to address gaps in some criminal justice systems to be more responsive to the rapid evolution of these crimes, as well as to develop certain laws.
4- Building and strengthening national capabilities helps in confronting these crimes, especially in the field of artificial intelligence.
5- Enhancing international cooperation among all different judicial, legislative, media, academic, and security bodies to develop joint, effective preventive plans and policies to combat these crimes. The results showed that the Cyber Security Authority contributed to raising citizens' awareness of

**cybercrime techniques, especially since Saudi citizens rely heavily on smartphones:**

- The Authority was able to inform citizens with awareness information about cybercrimes.
- Organizing conferences and seminars that highlight the Authority's efforts in combating cybercrime and explain the latest developments in raising awareness about these crimes.
In light of the above, the study concluded with a set of recommendations that support the contribution of the Anti-Cybercrime Authority in reducing cybercrime, in line with the Kingdom's Vision 2030:
- Enhancing knowledge about cybersecurity.
- Assessing risks and establishing effective preventive mechanisms to address rapidly evolving cybercrimes.
- Increasing public awareness campaigns to educate citizens on the importance of protecting their personal data.
- Enforcing legislation and regulations to combat these crimes by establishing more specialized courts.

Based on the study's findings, which included an analysis of studies conducted on cybercrime in the Kingdom of Saudi Arabia, available statistics on the Anti-Cybercrime Authority's contributions, and interview evidence, the researcher reached the following conclusions:
1- The Authority has contributed to raising public awareness, as citizens' understanding of its role encourages them to report incidents immediately.
2- The availability of a national internet browser has contributed to building public trust. 3- Studies have shown that despite citizens' reliance on smartphones, the Authority has played a significant role in warning them about cybercrime.
4- Awareness programs broadcast through social media have contributed to raising awareness about these crimes, particularly those committed via email.
5- Some studies have emphasized the need to organize (remote) awareness programs about cybercrime, presented by technical specialists.
6- The Cybercrime Law has contributed to building trust in the validity and security of electronic transactions, signatures, and records.
7- The use of electronic records has contributed to reducing these crimes.

The results of the interview guide revealed that the most common issues related to cybercrime include eavesdropping, threatening individuals, unauthorized access to websites, invasion of privacy through defamation, misappropriation of funds through illegal means, creating websites to promote prohibited substances, and fraudulent competitions.
- Regarding the Authority's contribution to reducing these crimes, it has implemented numerous awareness programs, sent text messages to mobile phones to educate citizens, held seminars in public gatherings, and established a hotline for reporting any threats. - Monitoring threats by issuing security alerts to citizens and informing them how to deal with them.
- International cooperation through joint cooperation protocols.
- Raising awareness about the dangers of cybercrime and how to prevent it.
- Launching several initiatives, including audio awareness messages, especially for the elderly.
- Implementing awareness programs presented by cybersecurity specialists.
- Incorporating a section on the role of security personnel in protecting members of society from cybercrime into the education curriculum.
- Establishing a cybersecurity unit within educational institutions to educate young people

about the dangers of cybercrime and how to protect themselves from falling victim to it.
- Adopting an incentive policy for employees to develop their cybersecurity skills.
- Leveraging digital transformation to build a supportive electronic knowledge environment for preparing cybersecurity specialists in light of the requirements of the modern technological revolution.

**The most prominent crimes dealt with by the Anti-Cybercrime Authority in the Kingdom of Saudi Arabia:**
1- Extortion and threats: Publishing private information or demanding ransom online. 2. Cyber fraud and identity theft: Deceiving individuals to obtain sensitive information (financial or personal) or using another person's identity. Hacking and unauthorized access: Gaining unauthorized access to websites, systems, or accounts to alter, damage, or steal data.
3. Defamation and slander.
4. Invasion of privacy.
5. Spreading malware.
6. Cyber espionage.

**The study identified several implementation mechanisms for the National Cybersecurity Authority's contributions to reducing cybercrime, including:**
- Strengthening the institutional capacity of the National Cybersecurity Authority enabled it to confront cyber threats and repel attacks.
- Recognizing cyberspace as an integral part of the Kingdom's national security, the Authority focused on developing qualified personnel to address these threats. Recent international reports have confirmed the Kingdom's advanced ranking in combating cybercrime.
- Playing an effective role in raising citizens' awareness of their personal information security through programs implemented via social media, traditional media, and various educational institutions.
- The Anti-Cybercrime Law, issued by Royal Decree on March 8, 1428 AH (corresponding to 2007 CE), established penalties for each crime and identified the competent authorities.
The study's general findings, derived from interviews and content analysis, are presented in the following tables:
Table illustrating emerging cybercrime methods:

| style | M |
|---|---|
| .Using phishing and spyware programs to steal data and blackmail others | 1 |
| .Using tools and techniques to encrypt sensitive data in order to hide it or exploit it illegally | 2 |
| .Hacking and breaching the security systems of governmental and private institutions | 3 |
| .Hacking applications and cloud services and seizing their content | 4 |
| .Spreading viruses and malware to block or disrupt vital services provided to citizens | 5 |

A table illustrating the reasons for the spread of cybercrimes:

| the reason | M |
|---|---|
| .Lack of public awareness of the dangers of cybercrimes and methods of preventing them | 1 |
| .The continuous increase in the number of users of modern technology | 2 |
| .The media's role in raising awareness and reducing the risks of cybercrime is weak | 3 |

Table (3): Perspectives on reducing cybercrime:

| Point of view | M |
|---|---|
| .Continuous updating of digital infrastructure and technical systems | 1 |
| .Forming specialized emergency security teams to protect against cybercrimes | 2 |
| .Intensify awareness programs for citizens on the safe and optimal use of digital platforms | 3 |
| .Continuous training of security personnel to keep up with technological developments | 4 |
| .Developing effective means and mechanisms to track perpetrators of cybercrimes | 5 |
| .Developing academic programs and creating curricula specific to e-citizenship | 6 |

Table (4): Contributions of the Cyber Security Authority:

| Contribution | M |
|---|---|

| | |
|---|---|
| .Creating positive attitudes among citizens towards the safe use of the Internet | 1 |
| Raising public awareness and motivating institutions to follow information security .standards | 2 |
| .Explaining methods of prevention and protecting society from the dangers of cybercrime | 3 |
| Achieving integration and coordination with various community entities to reduce .cybercrimes | 4 |
| .Preparing and developing programs and plans to address the phenomenon of cybercrime | 5 |

5): General proposals

| Proposal | M |
|---|---|
| .Activating a website that explains the legal penalties for perpetrators of cybercrimes | 1 |
| Issuing awareness booklets and brochures, especially in schools, to protect young people from .the negative effects of cybercrimes | 2 |

A table outlining proposals specific to employees in the security sector:

| Proposal | M |
|---|---|
| .Transferring international experiences and expertise in the field of combating cybercrime | 1 |
| .Increased training in artificial intelligence and cybersecurity technologies | 2 |
| Supporting young leaders and giving them the opportunity to build their technological .capabilities | 3 |
| .Establishing effective partnerships with technological universities within the Kingdom | 4 |
| .Encouraging outstanding talents and highlighting their achievements at the community level | 5 |

A table outlining the recommendations:

| Recommendation | M |
|---|---|
| Continued intensive awareness campaigns about the dangers of cybercrimes in schools, .universities, institutes, charities and all state agencies | 1 |
| .Expanding the use of artificial intelligence technologies to reduce cybercrime | 2 |
| .Continued awareness campaigns on cybercrimes carried out by the competent authorities | 3 |
| Attention should be given to academic research that focuses on innovative programs in .combating cybercrime | 4 |
| Encouraging interdisciplinary studies that combine different disciplines to arrive at effective .means of protection and investigation | 5 |

A table illustrating mechanisms for raising digital awareness among different segments of society:

| The mechanism | The symbol |
|---|---|
| .Implementing awareness programs through various media channels | A |
| Activating the role of schools and universities through meetings and awareness .campaigns | B |
| .Launching ongoing online awareness campaigns across digital platforms | C |
| Establishing partnerships with other countries and exchanging expertise in the field .of cybersecurity | D |

A table outlining recommendations for improving weaknesses:

| Recommendation | M |
|---|---|

| | |
|---|---|
| **Strengthening security cooperation between Arab countries in the field of combating cybercrime.** | **1** |
| **Transferring the expertise of developed countries to the Kingdom of Saudi Arabia, especially for those working in systems protection, police officers, criminal investigators, and information technology experts.** | **2** |
| **Utilizing artificial intelligence technologies to support future decisions in combating emerging cybercrimes and predicting their methods.** | **3** |

**First: Arabic References**

**A- Theses, Books, and Periodicals:**

1. Al Jarallah, Abdulaziz bin Mohammed. (2017). Cybercrimes and Their Penalties According to the Saudi Anti-Cybercrime Law. Riyadh: University Book House, 1st Edition.
2. Al Rabeeah, Saleh bin Abdullah. (2017). Digital Security and Protecting Users from Internet Risks. Riyadh: Communications and Information Technology Commission.
3. Al Shehri, Ali bin Mohammed. (2019). A Strategic Vision for Reducing Cybercrimes to Enhance Cybersecurity in the Kingdom of Saudi Arabia. PhD Dissertation, Naif Arab University for Security Sciences, College of Strategic Sciences, Kingdom of Saudi Arabia.
4. Al Shehri, Mohammed Riyadh. (2020). A Forward-Looking Vision for National Security in Light of Vision 2030. Unpublished PhD Dissertation, Naif Arab University for Security Sciences.
5. Al Omari, Sumaya Mushrif Abdullah. (2024). Cybersecurity and Its Role in Raising the Level of Public Security in the State – The Kingdom of Saudi Arabia as a Model.
6. Al Alwan, Jaafar Ahmed. (2022). Roles and Challenges of AI-Based Cybersecurity: A Case Study. Jordanian Journal of Business Administration, Vol. (18), No. (3), Jordan.
7. Al-Mutairi, Abdul-Ilah bin Mohammed. (2018). The Role of Media in Raising Awareness of Cybercrimes. Master's Thesis, Naif Arab University for Security Sciences, College of Social Sciences, Kingdom of Saudi Arabia.
8. Al-Maqsoudi, Mohammed Ahmed. (2017). Cybercrimes: Their Characteristics and How to Address Them Legally. Arab Journal of Security Studies, Vol. (23), No. (71).
9. Bin Amer, Walid. (2021). Cybercrime Against Childhood: A Crime That Challenges Reality and Outpaces Legislation. Algerian Journal of Security and Development, Vol. (10). Retrieved from: https://search.emarefa.net/detail/BIM-12H6184
10. Khaled, Nada Al-Merdas. (2023). Cybersecurity in the Kingdom of Saudi Arabia: Between Reality and Aspiration. International Journal for Publishing Research and Studies, Center for Leadership in Research and Studies, Jordan, Issue (49), Volume 5.
11. Abdulmohsen, Rana Misbah. (n.d.). Mechanisms for Combating Cybercrime in the Kingdom of Saudi Arabia. The Legal Journal, Issue (5).
12. Amara, Fathia. (2019). Cybercrime. Journal of Legal Research, Al-Tahadi University, College of Law, Issue (7), pp. 77–98. Retrieved from: http://search.mandumah.com/Record/102157
13. Latrach, Fairouz. (2016). Cybercrime in Algeria. Afaq Al-Uloom Journal, Ziane Achour University, Issue (1).
14. Mosaad, Mohammed bin Ahmed. (2019). A Strategic Vision for Combating Cybercrime to Enhance Human Security. Master's Thesis, Naif Arab University for Security Sciences, College of Strategic Sciences, Kingdom of Saudi Arabia.
15. Experts Authority. (1428 AH). Objectives of the Anti-Cybercrime Law, issued by Royal Decree No. (M/17) dated 8/3/1428 AH. Retrieved from the Experts Authority website: https://www.bae.gov.sa
16. National Cybersecurity Authority. (2024). Contributions of the Cybersecurity Authority. Accessed: 1/1/2024. Available at: https://www.my.gov.sa/wps/portal/snp/agencies/agencyDetails/ACH03
17. National Information Center. (2020).

**Second: Foreign References**

1. Forester, T. (1989). Essential Problems of the High-Tech Society. Cambridge, Massachusetts.
2. Ganesh, S., Ganapathy, D. H., &Sasanka, K. (2020). Awareness of cybercrime on social media. Journal of Contemporary Issues in Business and Government.
3. Heinonen, K. (2018). Consumer activity in social media: Managerial approaches to consumers' social media behavior. Journal of Consumer Behavior, Vol. 10, No. (6).
4. Jaishankar, K. (2008). Space Transition Theory of Cyber Crimes. Raksha Justice Programs.

5. Monni, S. (2018). Investigating Cybercrimes' Pervasiveness and Perception of Social Security. MA Thesis, Shahjalal University of Science and Technology.
6. Mshana, J. A. (2018). Cybercrime: An empirical study of its impact on social security in Tanzania. International Review of Law, Computers and Technology.