The Crime of Electronic Fraud: A Sociological Approach

Dr. Mahmoudi Reguia[1]

Dr.Mebrouk Meriem[2]

Dr. Guedouh Nourelhouda[3]

[1]Yahia Fares University of Medea (Algeria)

[2]Ali Lounici University of Blida (Blida 2 University), Algeria

[3]Yahia Fares University of Medea (Algeria)

Abstract

This research paper aims to define electronic fraud as a type of cybercrime that showcases the cyber risks the world is experiencing in the light of modern techniques and information and communication technologies, by targeting automated data-processing systems within a virtual environment "Computer and Internet", with the sole aim of achieving illegal material profits using fraudulent methods that show technical knowledge and information control skills, and the severity of the crime reflects the extent of its implications on individuals and institutions.

In this article, we start by identifying electronic fraud and defining the characteristics of the cyber offender involved in it, then, review the most common techniques used to commit this crime backed up by citing some concrete cases,and finally, we proceed to analyze the underlying factors of cybercriminal behavior, and provide a sociological analysis of cyber fraud from the Risk Society theory and the Routine Activities theory's perspective.

Key words:Electronic fraud,cybercriminal, information organization, Risk Society.

E-mail :[1]mahmoudi.reguia@univ-medea.dz, [2]m.mebrouk@univ-blida2.dz, [3]guedouh_houda@hotmail.com

Tob Regul Sci. ™ 2023;9(1): 2661-2675
DOI: doi.org/10.18001/TRS.9.1.184

Introduction:

Durkheim viewed crime as an integral part of society, it manifests in varying amounts depending on a society's social, economic, political and cultural conditions. Crime serves as a reflection of social reality, interacting with its numerous variables and adapting to various elements of development. The 1980s saw the advent of an information-based, technologically advanced world that has been significantly impacted by advances in informatics and technology.

[1] Principal auther

Automation of data transmission and storage, use of computer networks and the Internet have all revolutionized various sectors such as the economy, but have also provided criminals with greater opportunities to commit crimes. In essence, "modern information technology has increased the potency of crime".

This technological advancement in the ICT sector and the reliance on information systems and computer and Internet networks has caused new criminal patterns to emerge, known as "information crime" targeting individuals and financial institutions, for profit and wealth.

Electronic fraud is an economic crime against funds (Jafar, 2013, p. 156), an evolving type of fraud where electronic data processing systems are misused for financial gain or assets resulting from the use of keys, codes and electronic guides (Chouili, 2018, p. 136). It is typically performed by criminals, with a high level of technical expertise, focused specifically on the financial sector in an effort to obtain wealth quickly. In response, various international laws have been put in place to criminalize acts of cybercrime and classify them among core crimes for the losses it has caused which have exceeded millions of dollars, including Recommendation 89/9 from the European Council (Al Husseini, 2019, p. 273).

This criminal act has shifted from physical acts to online ones, with victims ranging from people to institutions. As such, this phenomenon should be analyzed as a digital criminal act from both a macro (Risk Society) and micro (Routine Activities Theory) level when approaching it sociologically.

Chapter One:Identifying the Electronic FraudCrime

I- Definition of electronic fraud

Cyber fraud is made up of two components: fraud, which is the unlawful acquisition of another person's assets, and electronic, which is used to express the notion of the computer part or the information era (Chouili, 2018, p. 135), forming one of the many types of fraud.

Electronic fraud as a cybercrime is defined by two criteria: legal, "consisting of criminalized conduct and the means used, and personal, containing the characteristics of the perpetrator, particularly with regard to knowledge of the perpetrator's technical know-how, and comprehensive definitions incorporating the multiplicity of criteria, " the object of the crime, its patterns, and the mechanisms by which it is committed."

Accordingly, we state the following: in its definition, cyber fraud is the "Unlawful activity to copy, alter, delete, transfer, rechannel or access information stored inside the computer, and it is limited here to identifying the characteristic of the criminal act only. It was defined by Tiedemann as:" All forms of unlawful conduct committed using the computer ", (Al jabouri, 2018, p. 25) focusing on the means of criminal act that include any computer that provides the offender with access to the Internet which is an important link between the potential targets of

fraud such as "private financial institutions that have introduced cybersecurity systems to secure themselves or at least reduce their losses if and when they fall victim to fraud."

Cybercrime is also defined as an offence committed by the authorized or unauthorized person using the computer, - for there is a relationship between the cybercriminal and the victim-, to manipulate the information system by stealing or corrupting data by using the latest virus technology and other methods of data destruction and software hacking, with the aim of achieving financial benefit. it was also defined as: "A new type of fraud where computers are misused in electronic automated data processing systems to acquire funds or assets illegally" (Chouili, 2018, p. 132)and make a profit, resulting in a financial loss to the victim, and the use of computer was a means of committing, facilitating or expediting fraud (Al-Jabouri, 2018, p. 29).

It was defined as: "Fraudulent behavior that uses computing methodologies (computing is based on the use of technical means to manage and process data and carry out tasks related to computer science and logic, "www.arablaw.org source website" Younes Arab's Internet and Computer Crimes book), with the intention of obtaining a financial privilege, namely intentional manipulation of information and data representing material values stored by the computer system, or the unauthorized introduction of valid information and data or the manipulation of data and commands controlling the programming process and any other means that would affect the computer in order to perform its operations on the basis of such data, commands and instructions in order to gain an unlawful profit of others".(Al-Shalabi, p. 40).

This definition included referring to electronic fraud as fraudulent behavior, detailing the nature of data and its procession through computer, as well as the specificity of the fraudulent money.The 1998 Model State Computer Crimes Code, adopted by the American Academy, classifies cyber fraud within the spectrum of fraud and theft, defining it as: "Manipulation of data and systems and use of computer to obtain or use other people ' Jaafar, 2013, p. 93), focusing e-fraud patterns.

According to the UNODC report, “cyber fraud involves using a computer for deception in order to gain money or other material benefits. Specifically, it is the manipulation of computer systems to generate false data, altering bank software for the purpose of transferring money illegally, and changing content in emails or text messages to scam people and steal personal information”, February 2013, p. 365. This definition outlines the major electronic fraud trends that can target both individuals and institutions, with the goal of obtaining illicit funds through automated data processing using a computer.

Electronic fraud is different in that it relies on "computers and the internet, as well as a person's technical knowledge of information systems, automated data processing, and the internet to commit fraud. This type of fraud is primarily targeted at individuals", banks, financial institutions, and companies that rely heavily on electronic funds transfers and bank deposits.

Electronic fraud in Algerian legislation has the same concept as fraud as defined in the Penal Code's Article 372, which explains and details the act of fraud, with the difference being the means used - computers and the internet. This is connected to the concept of cybercrime, i.e. crimes related to information and communication technologies, through Order 66/156, Section 7 (repeated) which concerns the automatic processing of data, Articles 394 to 394 (7) which include tampering with data processing systems (Lahcene, 2018, pp. 32-33). Therefore, all actions related to these systems, such as unauthorized access, staying or disrupting the system, intentional attacks on the system, and manipulation of data obtained from computer system crimes, are all classified under the same category.

A comprehensive definition of electronic fraud can be formulated as a deceptive act carried out through the use of modern technology, such as computers and the internet. This type of crime involves a range of intentional actions, including the manipulation of data and information that represent a material value stored in an information system, the input of unauthorized data and information, and the manipulation of programming instructions or any other means that can cause damage or intentional harm. Such actions may adversely impact a computer's ability to perform operations based on such data, instructions or orders, with the ultimate aim of obtaining illegal profit.

II- Characteristics of the Cybercriminal in Electronic Fraud

The term SKRAM expresses the total characteristics that distinguish the cybercriminal, where it refers to the Skill, Knowledge, Resources, Authority, and Motive (Jaafar, 2013, p.107).

1- **Skill:** The cybercriminal acquires it through practical experience or specialized study in the field of information technology or through interaction with others. It is worth noting that 60% of cases of electronic fraud, such as data manipulation, do not require technical IT skills, and cases carried out by specialists in this field are rare due to the difficulty of detecting program manipulation (Al-Jubouri, 2018, p.33).

2- **Knowledge:** The cybercriminal must have a comprehensive understanding of the crime, including the circumstances, details, likelihood of success, and potential failure. They can execute their crime on information systems similar to those they target before they carry out their crime.

3- **Resources:** Such as computers and supportive software.

4- **Authority:** This can be in the form of access codes to computer systems or gaining access to stored files and copying, modifying, destroying or stealing them. Cybercriminals have the authority to deal with data in the input, output, and storage stages, and convert this manipulation into illegal monetary gain (Al-Jubouri,2018, p.34).

5- **Motive:** It may be to achieve financial gain, to seek revenge against the target, either materially or morally, or to dominate the information system and overcome the complexity of technical means (Al-Husseini, 2019, p.63).

The cybercriminal who commits electronic fraud is a criminal who engages in an illegal act that requires punishment, and may be either authorized or unauthorized to use a computer and access its system. However, most cases of fraud are committed by insiders, as indicated by a German study revealing that 90% of detected manipulations were committed by employees of victimized organizations. Similarly, a study conducted by the New York Institute in 1983 revealed that 3/4 of electronic fraud cases, and in Sweden, 81% of fraudsters are affiliated with the victimized institutions. Hence, electronic fraud is also known as an in-house offense(Al-Momani 2010, p. 189).However, with the increasing use of Remote Access computer systems and ATMs, it is evident that:

- The number of cases of fraud by individuals outside the victim organization will significantly increase.
- With the advancement of security measures in the field of computer technology and their widespread use, cases of electronic fraud that do not rely on high technical skills will be limited to a narrow range, to be replaced by cases that require advanced skills. (Al-Jubouri, 2018, p.34).

According to studies conducted on electronic fraud perpetrators, there are several common characteristics and traits that they share. These include the following: (Al-Jubouri, 2018, pp. 34-35)

- The majority of electronic fraudsters have no criminal records.
- They hold positions in victimized institutions.
- Most of them do not possess high technical skills, but instead discover vulnerabilities through their use of computers.
- They are aged between 18 and 30 years old, and most of them are males.
- They have generally moderate moral values.
- They commit electronic fraud in order to achieve illegal financial gain or to show off their technical abilities and skills.

III- Methods of electronic fraud

The methods of electronic fraud have diversified and evolved in tandem with advancements in information and communication technology. The prevalence of electronic financial transfer systems has played a role in the growth of this crime and the development of its methods, particularly with the increase of specialized programmers in the field of information systems. So, what are the most important technical methods used in electronic fraud? We will then present examples that highlight the distinct characteristics of this crime.

1- Input manipulation:

62% of electronic fraud cases detected in the UAE in 1984 involved input manipulation, which refers to the act of altering data before or during its entry into a computer system. (Al-Mumani

2010, p. 190) This may involve inputting false information, changing data without deleting it, deleting parts of the information, or by concealing the information's true nature, as well as by manipulating data through unauthorized access. In most cases, the perpetrator responsible for collecting, examining, reviewing, and entering data into the computer system is from the same institution. (Al-Jubouri 2018, pp. 86-88)

2- Program manipulation:

It is a complex method that requires expertise and technical knowledge in the field of programming. It is considered one of the most dangerous forms of electronic fraud and one of the most detectable methods.

Manipulation of programs can be done through:

A- Manipulating the already implemented programs within the victim organization by introducing unauthorized modifications. Many programs undergo some modifications to correct them after their preparation and testing, which allows the possibility of introducing changes that would help the perpetrator in carrying out their crime through the use of malicious programs, "viruses".(Al-Moumani, 2010, p.193) For example, the Melissa virus, invented by David Smith, resulted in severe financial losses of over $80 million. (Yousif, 2018, p.68)

B- The utilization of extra software that could either be detected by the offenders themselves or already designed in advance to alter the computer's data through direct adjustments made in the computer's memory. Additionally, programs are employed during emergencies to surpass unbiased security protocols. (Al-Jubouri, 2018, p. 88).

3- Remote data system manipulation:

The increasing use of remote data processing systems in recent years has had an impact on the development of various methods used in electronic fraud. Remote manipulation through the end terminal, regardless of its location, has made fraud easier and more difficult to detect. It requires a computer connected to the central processing unit via a telecommunications network or other means of communication for the perpetrator to carry out the crime from their home, using their terminal unit without the need to enter the victim's organization (Al-Momani, 2010, p. 195). This is a more convenient method for illegal electronic financing.

4- Improper Use of a Code to Access a Paid System:

Using an incorrect code to access a paid system refers to the unauthorized entry into a paid information system by using a code that belongs to another person or a code owned by the system itself, which is considered invalid when used by an unauthorized person. This type of fraud is considered a violation of the system's terms of use and can result in legal consequences for the perpetrator. (Al-Mumani, 2010, p. 196)

Famous cases of electronic fraud according to the methods of commission (Samir Salman Al-Jubouri, 2018, pp. 130-141)

Method	Cases	Cybercriminal	Details	Consequences
Input manipulation	01	A programmer at a Swiss bank manipulated external bank transfers, obstructing information from performing its function	The instruction was to enter the actual value of the transfer multiplied by 1000, and the transfer was to a value of 98% of 1 million German Marks, for example, from Frankfurt to their partners in Switzerland, which means that they withdrew the equivalent value of this amount in Swiss currency multiplied by 1000.	The perpetrators were able to seize 700,000 Swiss francs from the bank's funds.
	02	Recruitment of a number of USA bank employees by criminal groups in 1971.	Entering incorrect data regarding the credit status of certain individuals, erasing files indicating bad credit histories and replacing them with false ones that do not reflect the truth in exchange for $50 for each case. If one of the institutions investigates the credit center of one of its clients, the information obtained will not be accurate.	The bank in California suffered losses of 200,000 dollars as a result of granting loans to individuals with poor credit scores.
	03	06 people	The perpetrators are "3 employees of the dog racing track in Florida, along with 3 employees of the institution responsible for equipping the track with computers. They manipulated the computer data in a later stage before extracting the data.	The theft of one million dollars from betting funds.

Program manipulation	01	A programmer at one of the USA banks.	The bank's account management software was altered using the "Salami technique," which involves deducting small amounts from several accounts and transferring the funds to one individual. Any excess expenses were then recorded in a separate account under the name Zzwiche. The operation was uncovered when the bank attempted to recognize its most recent customer in alphabetical order, only to find that the person with the pseudonymous account did not exist.	Obtaining hundreds of dollars monthly.
	02	A programmer at a major company in Germany in 1978.	The programmer used a specially developed program to carry out the fraud by inputting information related to fake individuals' salaries into the computer's memory that contains all salary information. He then entered a personal account to which these fictitious salaries were transferred. To avoid detection, he made modifications to other software that dealt with the payment of salaries, company account statements, and budgeting.	The embezzlement of 193,000 German marks before being accidentally discovered and prosecuted.

Remote data system manipulation	01	A software expert at an American bank	He was an expert programmer at an American bank and managed to access the bank's transport connection room. He obtained the code used by the bank and called the bank's information network using his phone, using the obtained code. He then planted a virus in the network whose mission was to transfer financial amounts from customer accounts to his own account in New York.	
Improper Use of a Code to Access a Paid System	01	The Gold and Schifreen case	They were able to obtain the special code issued by the British Telecommunications Regulatory Authority for one of its engineers to access their electronic information system, the Prestel System. This system provides subscribers with a database and information for a general system access fee, in addition to a cash payment that varies depending on the amount and format of the required information.	Using the code, we were able to access the system and obtain the desired service without incurring any expenses.

➢ From reviewing some of the cases that occurred in the early 80s, when the information revolution was in its infancy and was limited to American and European societies, before information and communication technology (ICT) became widespread in most countries of the world, taking into account the digital divide between the knowledge society that produces and controls knowledge, and the third world societies that consume technology. In addition to the fact that the use of ICT and its rapid and evolving development has infiltrated various fields, it is undoubtedly that the development in the world of modern technology has produced new methods and patterns in the technology world and led to the emergence of new criminal patterns over decades until our present time, especially with the development of software and the direct increase in electronic crimes and cyber-attacks. For example, the 2017 WannaCry virus spread in 120 countries around the world, causing significant losses within the information systems of government institutions, economic sectors, and private industries. (Youssef, 2018, p.68)

- Cyber fraud is perpetuated by proficient criminals who possess technical expertise, including programmers, computer experts, and individuals with a certain level of technical expertise who have employed it in electronic fraud crimes, most of which targeted financial institutions, such as banks. Studies have shown that computer system analysts are at the forefront of information technology criminals, committing 25% of total crimes, followed by system programmers at 18%, then information technology experienced system users at 17%, then insiders at 16%, then non-employees of the victimized organization at 12%, and finally computer operators at 11%. (Youssef, 2018, p. 69)

- The electronic fraud crimes were committed both individually and collectively by users within and outside of the targeted institution, as well as through organized criminal activity by recruiting employees from within the targeted institution in exchange for illicit financial gain.

Chapter Two: Theoretical Approach to Analyzing Electronic Fraud Crime

I. The Risk Society Theory for Monitoring and Analyzing the Risks of Electronic Fraud

The global transformation map for the concept of the "Risk Society" was characterized by:

- A shift from the cognitive model of the industrial society to the cognitive model of the information society, which resulted in the emergence of new areas such as virtual space and the flow of information.
- A shift from modernity to globalization, which manifested itself in political, economic, and cultural globalization.
- This change is the result of global transformations in the fields of economy, politics, culture, knowledge, and technology.
- The emergence of a new model of national security, namely, cybersecurity, on the ruins of traditional one.
- The cultural values such as the global survey of values emerged and resulted in a new global consciousness marked by electronic crimes like piracy and database sabotage. (Yahyaoui, 2019-2020, p. 10-11)

According to Ulrich Beck, the Risk Society is a methodological approach to dealing with risks and uncertainties, and it was presented even before modernity. It examines how to prevent and manage risks, or rather, describes the production and management of modern risks. The theory of Risk Society analyzes the technological and technical risks, which means the information society (Fawzi, 2019, p. 105).

Anthony Giddens suggests that both external risks from nature and tradition, and artificial risks caused by humans, exist. Additionally, electronic communication has created virtual relationships and actions that have added to the development of a risk society, due to the potential danger they

pose. Furthermore, this has had a negative effect on social and practical connections - especially in intimate or professional relationships - due to the extended reach of virtual connections that go beyond temporal and spatial limits. Subsequently, this has put a strain on criminal networks and virtual security has been compromised. (Fawzi, 2019, p. 107)

Therefore, the modern and advanced information and technology society is characterized by information and communication technologies that have led to the development and popularization of new criminal activities driven by the ever-increasing Internet connectivity. Cybercrime is a notable example when it comes to criminal offenses related to data, fraud, phishing, and other cyber-attacks. The introduction of new technologies such as IoT, Blockchain, and Cloud Services has created an unprecedented interconnectedness between nations, corporations, and individuals – this in turn has amplified the risk of malicious cyber intrusions. Due to their intensity and level of danger, electronic threats have been recognized as one of the major systemic risks threatening the world's informational infrastructure (Banga, 2019, p. 7).

"Cyber Risk" encompasses both the likelihood of something going wrong within an organization's information systems, as well as any associated damage to its assets and reputation. This is a technical issue that has an impact on all areas of the business and can be managed or mitigated through risk management(Banga, 2019, page 13). Electronic threats, meanwhile, are potential electronic events that can cause harm to systems or the enterprise either from within or outside of the organization by individuals or institutions (Banga, 2019, page 14).

As for cyber risk management: "The aim of managing cyber risks is to influence human behavior, practices, technical controls, and interactions between machines. It aims to coordinate activities and processes to prevent any undesired consequences and outcomes" (Banga, 2019, p. 13). It is based on the assumption of "when will we be attacked as an enterprise? How many times have we been attacked? When can we continue to resist?" (Banga, 2019, p. 22).

Electronic fraud, as an electronic crime, targets information systems by manipulating data or programs directly, remotely or by using incorrect codes, malicious software, or phishing scams, which can be considered as electronic threats. These threats reflect the electronic risks facing the information systems infrastructure of victimized enterprises, which are the backbone of the information society, through the evolution of modern technological advancements and the creation of criminal opportunities within the electronic and digital environment. This highlights the global nature of the dangers, as risks and opportunities are distributed among individuals and major groups in the risk society.

- Risk management frameworks:

The risk society theory can be applied to manage electronic fraud risks through various risk management frameworks. Here are some examples:

A. ISO 31000:2018 - Risk management – Guidelinesis an international standard that provides principles and guidelines for risk identification, analysis, evaluation, treatment, monitoring, and review, and can be used to integrate the principles of the risk society theory in identifying and managing electronic fraud risks.

B. COBIT 5 is a governance framework that aligns IT with business objectives and provides guidance on risk management, control, and governance.

C. NIST Cybersecurity Framework that helps organizations manage and reduce cybersecurity risks by identifying, protecting, detecting, responding, and recovering from cyber-attacks.

D. FAIR (Factor Analysis of Information Risk) model provides a systematic approach to analyzing and assessing information security risks, and by applying the principles of the risk society theory, can be used to analyze electronic fraud risks and their potential impact on an organization.

II. The Routine Activity Theory (RAT) to explain electronic fraud

What are the underlying factors for committing criminal behavior in the cyberspace?

The Routine Activity Theory differs from other crime theories due to its innovative and distinct perspective on crime, criminals, and victims. It considers the actions of both offenders and victims which eventually leads to the crime being committed. The primary objective of this theory is to provide an in-depth understanding of the complex mechanisms of criminal conduct and the modus operandi of criminal activities. Therefore, the theory offers an alternative interpretation of criminal behavior, as it directs its attention not to the roots of criminal acts, but rather to the acts themselves (Soliman Ali M., 2022, p.116).

According to Lawrence E. Cohen and Marcus Felson (1979), three main elements are necessary for a crime to occur:

- A motivated offender: (with information knowledge "SKRAM"), is anyone and for any reason might commit a crime (R. V. Clarke and M. Felson, 1993, p 2).
- A suitable target:(Data) is any object(person or property) with a position in space and time that is likely to be taken or attacked by the offender(R. V. Clarke and M. Felson, 1993, p 2).

The following acronyms have been used to describe accessible targets:

• VIVA – Value, Inertia, Visibility, Access • CRAVED – Concealable, Removable, Available, Valuable, Enjoyable, Disposable,

- The absence of a capableguardian:who in most cases isn't a policeman or a security guard but rather neighbors, friends, relatives, bystanders, or the owner of the property targeted. This element is a reminder that the movement of physical entities in space and time is central to the approach (R. V. Clarke and M. Felson, 1993, p 3).

This theory consolidates various criminological analyses into a comprehensive framework that links legal and illegal activities and that serves as a useful tool for criminologists and law enforcement agencies in understanding and preventing criminal activities (Lawrence E. Cohen and Marcus Felson, 1979, p. 591).

Cybercriminal activity, as a routine or habitual activity, is one of the electronic activities generated by information system technologies and digital technologies, which reflects the electronic risks and threats witnessed by the information society.

Electronic fraud is facilitated by criminals with a proficient understanding of digital technologies, who are able to manipulate data, programs, and other methods to cause damage to an information system for illegitimate financial gain. With the prevalence of modern tech advancements, alongside malicious software specifically designed for these purposes, electronic fraud is seen as a profitable endeavor that carries few risks and a low detection rate on the part of victims. Criminals who are highly specialized or affiliated with criminal groups are particularly successful in utilizing malicious software to attack information systems.

The RAT approach aims to explain why a person is victimized or offended by explaining how their routine activities and the daily patterns of their social behavior bring them into contact with situations conducive to crime (Per-Olof H. Wikström, 2011, p5).

As for individuals, with the increasing use of direct electronic services such as online banking, e-commerce, social networking, and file sharing, users are vulnerable to phishing attacks or fraud. Social media platforms such as Facebook and Twitter also provide a ready-made framework for potential victims of fraud, reaching millions of targets.

Conclusion:

In conclusion, electronic fraud is a crime that primarily targets digital data and takes place within information systems, making it tricky to address the actual consequences. The evolution of this type of fraud has been encouraged by modern technology, specifically malware. Moreover, it results in many losses, not only material or environmental but also on individuals and institutions, such as those in the financial sector with losses exceeding millions of dollars. Therefore, it is critical to enact legal regulations and international agreements to adapt laws accordingly. It is also vital to put cybersecurity measures into practice in order to secure digital infrastructure and protect online privacy through countermeasures and security measures.

List of References

References in Arabic

1. Al-Jubouri, S. S. (2018). Electronic Fraud Crime: A Comparative Study. Beirut-Lebanon: Zain Legal and Literary Library.
2. Al-Husseini, A. A. (2019). Computer and Internet Crimes: Cybercrimes. Beirut, Lebanon: Zain Al-Huquqiah Publications.
3. Ash-Shalabi, F. A. (n.d.). Forms of fraud and forgery in credit cards. Arab Journal of Security and Training Studies, 29(85), 47-84.
4. Al-Moumani, N. A. (2010). Cybercrimes. Amman, Jordan: Dar Al-Thaqafa Publishing and Distribution.
5. Banga, A. A. (2019). Cybersecurity risks and their economic effects - a case study of the Gulf Cooperation Council. Development Studies (63).
6. Jafar, A. (2013). Modern information technology crimes against individuals and governments: a comparative study. Lebanon: Zain Law and Literary Library.
7. Raouf, O. (2016). Alexandria: Wafa Legal Library.
8. Shweili, A. M. (2018). Electronic fraud among university students. Al-Imam Al-Kadhim, 129-154.
9. Fawzi, A. (May 2019). Cybersecurity: Sociological analysis of social and legal dimensions. National Social Magazine, 56(02), 99-136.
10. Lahcen, N. (2018). Investigation into information technology-related crimes between legislative texts and technical privacy. Tlemcen-Algeria: New University Press.
11. Crime, M. A. (February 2013). A comprehensive study of cybercrime. New York: United Nations.
12. Yahyaoui, N. (2019-2020). Lectures on the community risk scale. Kheider Mohammed Biskra University: http://elearning.univ-biskra.dz/moodle2019/mod/resource/view.php?id=29278.
13. Youssef, M. (2018). Crimes of tampering with data processing systems: their nature, forms and international efforts to combat them - a comparative study. Algeria: Dar El Khaldounia.

English references

1. Soliman Ali M. (October 2022). Contribution of Routine Activities Theory to Understanding Cybercrime: An Exploratory Study.
2. L. E. Cohen, M. Felson (August 1979). Social Change and Crime Rate Trends: A Routine Activity Approach.American Sociological Review, Vol. 44, No. 4 (Aug., 1979), pp. 588-608.
3. Per-Olof H. Wikström (2011). Routine Activities Theory. Cambridge university.
4. R. V. Clarke and M. Felson (1993). Routine Activity and Rational Choice Volume 5.
5. State of New South Wales through the Department of Attorney General and Justice (2011). Routine Activity Theory: Crime preventionfactsheet.
6. M. Edwards, E. Williams, C. Peersmanand A. Rashid (February2022). CharacterizingCybercriminals:AReview. University of Bristol.

7. International Organization for Standardization. (2018). ISO 31000:2018 Risk Management-Guidelines.
8. ISACA. (2012). COBIT 5: A business framework for the governance and management of enterprise IT.
9. National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity.
10. Factor Analysis of Information Risk (FAIR) Institute. (2020). FAIR model.