



Akademik Eğitim ve Sosyal Bilimler Dergisi (AJESS Journal)

Cybercrimes: A Descriptive-Analytical Study

Dr. Tarafi Sadek, University of Bouira, Algeria

s.tarafi@univ-bouira.dz

Dr. Djemaa Mohamed, University of Bouira, Algeria

mohamed.djemaa@univ-bouira.dz

Article History

Received: 31/07/2026; Accepted:16/09/2026 ; Published:09/10/2026

Abstract:

Through this research paper, we seek to identify a new crime in Algerian society, which has begun to spread in a striking manner. This crime is a product of digital and technological development, as it is committed through the Internet and using modern technologies, which is known as electronic crimes. Our study aims to know the nature of these electronic crimes and their most important classifications

Keywords: Electronic crimes, Technological development, Fraud, The Spying.

Introduction:

Cybercrime is considered one of the most serious emerging problems in Algerian society. In recent years, it has witnessed a significant increase, particularly with the widespread use of social media, making everyone vulnerable to becoming a victim of one of these crimes. Such crimes have increasingly disturbed and disrupted the lives of Internet users and have become a persistent concern that threatens the security and stability of society.

“Cybercrime is any unlawful, unethical, or unauthorized conduct involving the automated processing or transmission of data” (Al-Shukri, 2008, p. 113). It is a crime committed through electronic means with the aim of causing harm to individuals. Among its characteristics is the fact that it is perpetrated by professional cybercriminals through the Internet, using modern technologies and means with exceptional speed. It is also characterized by its covert nature, unlike traditional crimes, and by being transnational, meaning that it is not restricted by geographical boundaries. Based on this perspective, this research paper seeks to examine the nature of cybercrime and its main classifications.

1. The Nature of Cybercrime:

Cybercrime has distinctive characteristics and features that set it apart from traditional crimes. It is a “soft” crime, far removed from violence, force, and physical coercion, as it requires nothing more than a few keystrokes. It can also be committed remotely and at extraordinary speed, while proving its occurrence and establishing the identity of its perpetrators can be particularly difficult.

In this regard, Mahmoud Ahmed Ababneh states that: “These crimes are transnational, owing to the opportunities provided and made possible by modern communication technologies and computers. They also require the presence of a computer as a means of committing the crime, as well as technical knowledge of how to use it” (Ababneh, 2005).

Miftah Bou Bakar Al-Mutardi further points out that the perpetrator of cybercrime is generally socially well-adjusted and financially capable, and that his motive for committing the crime is often the desire to challenge or defeat the system rather than the pursuit of profit or material gain. By contrast, the perpetrator of a traditional crime is often socially maladjusted, and his primary motive is usually the pursuit of quick material benefit. (Al-Mutardi, 23–25/09/2012, p. 13)

1.1. Definition of Cybercrime:

Cybercrime is among the types of crime whose terminology has evolved and varied over time. It was formerly referred to as “computer misuse,” followed by terms such as “computer fraud,” “computer crime,” “computer-related crime,” “high-tech crime,” “hacker crimes,” and “Internet crimes,” eventually leading to the most recent term, namely “cybercrime” (Allah, 2017)

Cybercrime refers to criminal activity committed through the Internet using modern means and technologies, as well as through various search tools, communication platforms, and social media networks. A comprehensive definition of cybercrime was provided during the Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, where it was defined as follows: “Any crime that can be committed by means of a computer system or

computer network, or within a computer system, and includes, in principle, all crimes that can be committed in a digital environment” (Al-Mana’sa, 2001)

1.1. Characteristics of Cybercrime

Cybercrimes are characterized by a number of distinctive features that differentiate them from other types of crime. They are often considered “soft crimes” that are difficult to detect and whose perpetrators are difficult to identify. They are also transnational in nature, as they are not confined to a specific geographical area. Accordingly, the main characteristics of cybercrime can be identified as follows.

1.1.1. Transnational Nature

Cybercrime is not confined to a specific geographical area, as its perpetrator can commit the crime even from outside their country. The perpetrator may also conceal the traces of the crime and eliminate its evidence rapidly, which makes tracking and identifying them particularly difficult, especially due to the geographical distance separating the perpetrator from the victim.

Cybercrime is considered to have an “international dimension,” meaning that it is transnational in nature. It may cross geographical borders because its execution takes place through information networks, which often gives rise to legal, administrative, and technical challenges. It may also create political difficulties concerning efforts to combat it, particularly with regard to criminal prosecution procedures (Ataya, 2015, p. 374)

1.1.2. Difficulty of Detection

Cybercrimes are generally committed covertly and in complete secrecy, making both their detection and the identification of their perpetrators difficult. Data and information are transmitted in the form of electronic pulses. Moreover, such crimes are often organized, planned, and carried out across the territories of several countries through the use of the global communications network (the Internet). In addition, digital evidence of the crime can be destroyed within a very short period of time (Batli, 2015, p. 34)

1.1.3. Difficulty of Proving Cybercrime

Cybercrime is difficult to prove because it occurs within the realm of digital data through computers and the Internet, unlike traditional crimes. This makes it more difficult for security authorities to determine the constituent elements of the crime. Furthermore, the perpetrator can easily conceal or completely erase the evidence of the crime by simply pressing a single button and doing so almost instantaneously. The main factors contributing to this difficulty include the following: The difficulty of preserving its digital traces.

The high level of technical expertise required to detect such crimes, which may hinder the work of investigators who are accustomed to dealing with traditional crimes.

Reliance on deception in committing such crimes and on misleading techniques to conceal the identity of their perpetrators.

Reliance on a very high level of skill and intelligence in carrying out such crimes.

The temporal, geographical, and legal dimensions play an important role in dispersing investigative efforts and hindering international coordination aimed at tracking such crimes (Heroual, 2006, pp. 39–40)

1.1.1. Professionalism of Cybercrime Perpetrators:

Cybercrime perpetrators are generally characterized by intelligence and cunning, as well as a high level of technical expertise and extensive knowledge of the methods used in computer systems, including how to operate such systems, store information, and access it. In contrast, perpetrators of traditional crimes are often ordinary individuals with limited education or average educational backgrounds (Ataya, 2015, p. 373)

2. Classifications of Cybercrimes:

Cybercrimes generally require access to the Internet and an individual who is proficient in using computers. However, cybercrime perpetrators can be divided into several categories, as they differ from one another according to the nature and type of cybercrime committed. Accordingly, this section addresses some categories and types of cybercrime, such as cyber espionage, cyberterrorism, and organized cybercrime, as well as the categories of their perpetrators, including hackers, professional cybercriminals, and revenge-driven perpetrators.

2.1. Categories of Cybercrime Perpetrators:

2.1.1. Hackers:

Hackers are generally experienced programmers who gain unauthorized access to information systems and breach the security barriers protecting these systems. They can be divided into two types. The first consists of amateur hackers or individuals who engage in hacking activities for amusement. These are intruders and unauthorized users who challenge network security measures, although they generally lack motives related to challenge or self-assertion. This category largely includes pupils, secondary-school students, and unemployed young people.

The second type consists of professional hackers, who are individuals who infiltrate computer systems in order to access the information stored therein, damage or tamper with it, or steal it (Chaabane, 2009, p. 123)

2.1.2. Professional Criminals (Computer Professionals):

This category is characterized by extensive experience and a broad range of technical skills and expertise. Its members are also distinguished by their ability to organize and plan the activities they undertake. Therefore, they are considered among the most dangerous technology-related criminals. Their attacks are primarily aimed at obtaining financial gains for themselves or for entities that commission them. Some of their attacks may also be intended to achieve political objectives.

Members of this category can be classified into several groups. For example, there are professional industrial espionage criminals, whose activities are directed toward penetrating the computer systems of industrial companies and business enterprises with the aim of obtaining their confidential information and trade secrets, either for their own business interests or, more commonly, on behalf of competitors in the market.

There is also a category of fraud and forgery criminals, whose activities are primarily aimed at achieving financial gains and appropriating the funds of others. In addition to their distinctive technical knowledge, high level of organization, and careful planning of the activities they intend to carry out, members of this category are characterized by secrecy and discretion. They make every possible effort to conceal their technical methods and prevent the disclosure of the techniques they use to commit their crimes (Chaabane, 2009, p. 124)

1.1.1. The Vindictive (Revenge-Driven) Offenders:

This category is generally characterized by the absence of the objectives and motives of cybercrime typically found among other categories. They do not seek to demonstrate their technical capabilities or skills, nor do they pursue material or political gains. Rather, their activities are driven by a desire for revenge and retaliation, often as a consequence of the way they have been treated by their employer or by the organization concerned when they are not employees thereof.

Accordingly, they can be divided into two groups: system users, including employees, subscribers, or individuals otherwise connected to the system targeted by the crime; and outsiders who have reasons to seek revenge against the organization targeted by their activities. Members of this category are not characterized by advanced professional technical knowledge. Their activities predominantly involve the use of techniques such as introducing viruses, deploying malicious software, sabotaging systems, or damaging their data. This category is considered the easiest to detect in terms of its criminal activities, as its members are less dangerous than other cybercriminals. (Chaabane, 2009, p. 125)

1.2. Categories and Types of Cybercrimes:

1.2.1. Crimes Related to Individuals' Lives

Crimes related to individuals' lives vary in nature; however, they share a common objective, namely, causing harm and damage to individuals and compromising or destroying their data through the use of information systems and the Internet. Among the most prominent cybercrimes affecting individuals are defamation and insult, damage to the reputation of others, intimidation and harassment, identity theft, invasion of privacy, and defamation.

1.2.1.1. Insult, Defamation, and Damage to Reputation:

Insult and defamation are among the most common crimes committed over the Internet, as they affect the honor, dignity, and reputation of others. Such offenses may be committed through electronic communications, whereby, in accordance with the general rules governing insult and defamation offenses, the perpetrator uses obscene or offensive expressions that violate and undermine the honor of the victim.

With technological development, the Internet has become one of the principal means—if not the most widespread means—used to commit such offenses. Insulting and defamatory statements are commonly disseminated through websites and Facebook, making them accessible to anyone who visits the relevant site, where such content may be viewed or heard. The Internet constitutes an unlimited arena, as it receives and disseminates content without effective restrictions or prior control. Consequently, certain forms of misuse may result in harmful and abnormal practices, particularly when individuals are publicly defamed. (Ayad, 2007, p. 77)

The offender may publish information about the victim that is confidential, misleading, or inaccurate. The victim may be an individual, a community, or a commercial or political organization. (Al-Shawabkeh, 2004)

1.2.1.2. Invasion of Privacy and Defamation:

Privacy may be violated by publishing private information concerning individuals, accessing their electronic accounts and disclosing information about them, or collecting and publishing personal information relating to individuals. Defamation, on the other hand, includes the use and dissemination of private information or information relating to deviant behavior or criminal activity with the intention of assassinating an individual's character or causing harm to their reputation. (Ataya, 2015, pp. 32–33)

1.1.1.1. Intimidation and Harassment:

This refers to threatening another person with harm, with the aim of instilling fear by exerting pressure on an individual's will and making them fearful of the harm that may be inflicted upon them, their property, or persons associated with them. Threatening others through e-mail is considered one of the most significant forms of unlawful use of the Internet, whereby the perpetrator sends the victim an electronic message containing threatening or intimidating statements. This category also includes cyberstalking, which is carried out through e-mail or various forms of instant communication. Such stalking may involve threatening and harassing messages and shares with other crimes the objective of controlling the victim. However, it is distinguished by the ease with which the perpetrator can conceal their identity, in addition to the diversity and accessibility of means of communication over the Internet, which has contributed to the spread of this phenomenon (William, 2022, p. 224)

1.1.2. Crimes Related to Money:

Crimes related to money vary according to their nature; however, they all aim to obtain financial gains through the use of information systems. Among the most prominent cybercrimes related to money are the production and sale of drugs, as well as electronic fraud and scams.

1.1.2.1. Drug Production on the Internet:

A large amount of information related to drug production is disseminated through social networking sites and the Internet, including recipes, ingredients, and quantities. Such information is publicly available and accessible to young people,

adolescents, and drug users. However, this information is not necessarily accurate or reliable; it may be false or misleading, potentially exposing those who attempt to follow it to serious injuries, permanent illnesses, or, in some cases, even death. Moreover, production tools are available online, as are the chemicals required for producing narcotic substances, and these materials and equipment are often inexpensive (Al-Badayneh, 2011, p. 46)

1.1.2.2. Drug Sales on the Internet:

Drug dealers use the Internet to market and sell their products. Such transactions are often conducted through discussion boards and chat rooms using coded language, whereby drugs are shipped to the purchaser's address. Information necessary for producing drugs at home may also be provided (Al-Badayneh, 2011, p. 47)

1.1.1.1. Cybercrime of Online Fraud and Deception

These crimes are committed through the Internet using various carefully designed methods and forms with the aim of defrauding and appropriating other people's money. Among the most prominent forms are those carried out through social media platforms, as these platforms provide an easy means of manipulating others and obtaining their money unlawfully. Many users of such platforms have fallen victim to fraud and deception. Examples of online fraud and deception include fraud through network marketing, also known as e-commerce fraud; fraudulent job offers; fraud through online begging by appealing to people's sympathy; and fraud involving the dissemination of examination questions.

1.1.2. Crimes Related to State Security

Technological development has contributed significantly to the emergence and spread of these cybercrimes, thereby making all states vulnerable in terms of their security and stability. Contemporary warfare has become largely cyber-based, relying on espionage, hacking, and sabotage. Among the most significant crimes related to state security are espionage, cyberterrorism, and organized crime.

1.1.2.1. Cyber Espionage

Cyber espionage refers to accessing other people's information without their knowledge through the Internet and by using modern technological means, with the aim of causing harm to them and producing destructive effects on their electronic devices. Such activities may be motivated by the nature of the perpetrator, including political, religious, or racial motives. In accessing and stealing other people's data, the spy relies on "the use of programs that track and monitor the behavior of a device, from keystrokes to monitoring the websites visited by the user, with the purpose of stealing confidential information such as passwords or conducting surveillance. The primary function of spyware is to monitor and record all movements and actions performed on a computer. Once the program is installed on the computer, it conceals itself within the system, making it difficult for the user to detect its presence" (William, 2022, p. 226)

1.1.2.2. Cyberterrorism

Cyberterrorism is defined as "aggression, intimidation, or physical or psychological threats perpetrated by states, groups, or individuals against a person's religion, life, honor, intellect, or property without legitimate justification, through the use of information resources and electronic means in their various forms of aggression and manifestations of corruption. Terrorism relies on the use of scientific and technological capabilities and the exploitation of communication tools and information networks in order to intimidate and terrorize others, cause them harm, or threaten them with actions that may adversely affect them" (Youssef, 2011, pp. 219–220)

In this regard, Stark argues that cyberterrorism is "the deliberate use, or threat of use, of virtual warfare or virtual violence for political, social, economic, or religious purposes by state-supported groups or non-governmental groups, with the aim of generating fear, anxiety, and suffering within a targeted society" (Al-Badayneh, 2011, p. 12)

"Thus, the experience of Al-Qaeda and ISIS suggests the success of these two organizations in implementing their programs and achieving their objectives. This was accomplished through their reliance on social media platforms such as Facebook, Twitter, WhatsApp, Instagram, and other applications and new media platforms. The Internet and new media have enabled terrorist groups to engage in propaganda, recruitment, fundraising, communication, information gathering, internal communication, and the establishment of global networks of supporters and sympathizers" (Qirat, 2012).

1.1.1.1. Organized Crime

Organized crime refers to a criminal society operating outside the framework of the people and the government, comprising thousands of criminals who operate according to a highly precise and complex system that may surpass those adopted by the most developed and advanced organizations. Its members are subject to legal rules established by the organization itself, and severe sanctions are imposed on anyone who deviates from the group. In carrying out their criminal activities, members adhere to careful and well-planned strategies, through which they generate substantial financial gains.

An example of such crimes is car theft carried out by criminal gangs that use the Internet to identify locations where the prices of automobile spare parts are high. They then sell the stolen parts in those locations in order to secure the greatest possible profit (Moulay, 1–4 June 2010)

Conclusion

After examining the nature of cybercrimes and their main classifications, it has become clear that these crimes are diverse and vary according to their nature. They can be broadly classified into crimes affecting individuals' lives, crimes involving property and financial interests, and crimes threatening state security.

It has also become evident that these crimes have become a source of growing concern, disturbing the lives of Internet users and threatening the security and stability of human societies. This situation calls upon states to develop a serious and comprehensive defense strategy to confront the risks posed by these hidden and transnational crimes.

References

- 1-Ibrahim, R. I. (2015). Cybercrime and Ways of Combating It in Islamic Sharia and International Legal Systems: An Applied Analytical Study. *Journal of the Faculty of Sharia and Law in Tanta*, 30(2), 374.
- 2-Al-Badayneh, Z. M. (2011). *Youth, the Internet, and Drugs* (1st ed.). Riyadh, Saudi Arabia: Center for Studies and Research.
- 3-Al-Shukri, A. Y. (2008). Information Crime and the Crisis of Criminal Legality. *Kufa Studies Center Journal*, 5(7), 111–132.
- 4-Al-Shawabkeh, M. A. (2004). *Computer and Internet Crimes (Cybercrime)* (1st ed.). Amman: Dar Al-Thaqafa for Publishing, Distribution and Education.
- 5-Al-Mutairdi, M. B. (September 23–25, 2012). Cybercrime and Overcoming Its Challenges. *Proceedings of the Third Conference of Presidents of Supreme Courts (Cassation, Appeal, and Review) in Arab Countries*. Sudan.
- 6-Al-Mana'isa, A. W. (2001). *Computer and Internet Crimes*. Amman, Jordan: Dar Wael for Publishing and Distribution.
- 7-Batli, G. (2015). *Cybercrime: A Comparative Study*. Algeria: Algerian Publishing House.
- 8-Bin Gharam Allah, A. A. (2017). *Internet Crimes and Their Penalties under the Saudi Anti-Cybercrime Law, Followed by the Effects of Globalization on Internet Users*. Saudi Arabia: Dar Al-Nasher Al-Jami'i.
- 9-Shaaban, S. (2009). Cybercrime: An Analytical Approach to Defining the Concept of Crime and the Criminal. *Studies and Research*, 1(1), 124.
- 10-Ababneh, M. A. (2005). *Computer Crimes and Their International Dimensions*. Amman: Dar Al-Ilm wa Al-Thaqafa for Publishing and Distribution.
- 11-Ataya, I. R. (2015). Cybercrime and Ways of Combating It in Islamic Sharia and International Legal Systems: An Applied Analytical Study. *Journal of the Faculty of Sharia and Law in Tanta*, 30(2).
- 12-Ayyad, S. A. (2007). *Information Crime and Internet Criminality*. Alexandria: Dar Al-Fikr Al-Jami'i.
- 13-Qirat, M. (2012). Media and Terrorism: Between Patriotism, the Right to Know, and Blackmail. In *Proceedings of the Media and Crises Conference: Challenges and Prospects* (pp. 51–78). Sharjah: College of Communication, University of Sharjah.
- 14-Moulay, A. (June 1–4, 2010). The Difficulties of Electronic Administration in Algeria. *Proceedings of the First World Conference on Electronic Administration in the Mass Society*. Tripoli: Al-Madina Multimedia Center.
- 15-Harwal, N. H. (2006). *Procedural Aspects of Internet Crimes* (1st ed.). Alexandria, Egypt: Dar Al-Fikr Al-Jami'i.
- 16-Youssef, A. F. (2011). *Cybercrime and Information Crime and International and Domestic Efforts to Combat Computer and Internet Crimes* (1st ed.). [Alexandria, Egypt: Al-Wafaa](#) Legal Library.
- 17-William, A. (2022). The Risks of Electronic Violence on Young People: A Field Study. *International Journal of Humanities and Educational Research (IJHER)*, 4(4), 213–237.