

The New Dimension of Electronic Crime and the Specificity of Its Perpetrator

البعد الجديد للإجرام الإلكتروني وخصوصية مرتكبه

Mamene Besma *

, State Laboratory and Social Security: Health and Food Security. Abbas laghrour khenchela University

E-mail: mamen.besma@univ-khenchela.dz

The date of Submission : 2024/12/08

The date of revision:2026/01/20

date of publication:30-01-2026

Abstract:

In addition to the material and moral damages inflicted upon victims, these crimes negatively impact trust in digital systems and hinder economic development. Cybercrimes are highly diverse, including hacking, cyber extortion, identity theft, the dissemination of false news, and more. What adds to the complexity of these crimes is the profile of the cybercriminal, who possesses advanced technical skills that enable meticulous planning and avoidance of detection. This study aims to shed light on the personality of the cybercriminal, their motives, and their methods of operation, with the goal of gaining a deeper understanding of this phenomenon and developing more effective strategies to combat it. The study will focus on answering the following questions: What are the main motives behind committing cybercrimes? What technical skills do cybercriminals possess? And what are the most prominent methods they use to perpetrate their crimes

Keywords : Cybercrime, privacy, cybercriminal, criminal liability ,Punishment.

الملخص:

لقد شهد العالم العديد من التطورات في جميع المجالات والميادين خاصة المجال الإلكتروني فبعد ظهور الشبكة العالمية للإنترنت وبقدرة ما سهلت الحياة واختصرت الوقت والجهد في توفير المعلومة وتغيير نمط الحياة ، بقدر ما ساء البعض استعمالها مما ساهم في بروز طائفة جديدة من المجرمين تختلف عن تلك المعروفة والتقليدية. فالجرائم المعلوماتية أصبحت تشكل تهديداً متزايداً على الأفراد والمجتمعات والشركات والحكومات على حد سواء. فبالإضافة إلى الأضرار المادية والمعنوية التي تلحق بالضحايا، كونها تؤثر سلباً على الثقة في الأنظمة الرقمية وتعرق التنمية الاقتصادية. وما يزيد من تعقيد هذه الجرائم هو شخصية المجرم المعلوماتي الذي يتمتع بمهارات تقنية عالية تمكنه من التخطيط لعملياته بعناية وتجنب اكتشافه. ولهذا فإن هذه الدراسة تسعى إلى تسليط الضوء على شخصية المجرم المعلوماتي، ودوافعه، وأساليب عمله، وذلك بهدف فهم أعمق لهذه الظاهرة وتطوير استراتيجيات أكثر فعالية لمكافحتها.

الكلمات المفتاحية: الجريمة الإلكترونية، خصوصية ، المجرم الإلكتروني ، المسؤولية الجزائية ، العقاب .

* Corresponding Author :

Introduction:

Long ago, gangs appeared in roads and cities, and the latter were aimed at traditional crimes such as theft, kidnapping, vandalism etc., and the police used to deal with this type of crime until the advent of computers and the Internet, and these means began to be exploited in its negative aspect and committed several crimes through it, which are increasing as people use computers, and among these crimes are theft, extortion, etc.

These individuals target the infiltration of computer systems, email, or websites on the Internet, especially the websites of well-known companies like Microsoft and other global corporations, which are often targeted by competing companies. Such attacks can result in significant financial losses. They may also target bank websites with the aim of accessing customer accounts and stealing funds.

These crimes do not necessarily have to be committed by the criminal and the victim within the same country.

There may be a geographical dimension to this type of crime, where the perpetrator is in one country and the consequence is in another country or continent. This is what is called a technical criminal or a cybercriminal. The latter has a great deal of knowledge and expertise in the field of its use, which enables him to carry out his crime and work to avoid its discovery, as he can overcome many of the punishments he faces while committing the crime. This leads us to ask the following question: Who is the cybercriminal and how have countries dealt with this type of criminal?

1. The Concept of the Cyber Criminal

1.1- Definition of the Cyber Criminal and Demonstration of His Characteristics

Some have defined the **cyber criminal** as "every person who commits intentional acts constituting a positive or negative behavior by using information technology to create a criminal model by attacking a right or interest". The characteristics of the cyber criminal often resemble the characteristics of white-collar criminals (Hijazi, 2008, p 105)

Others have defined the information criminal in cybercrime as when we are not dealing with an ordinary criminal, but rather a criminal with technical skills and knowledge of the technology used in the automated calculation system.

From the above, we conclude that the cybercriminal is a person with exceptional expertise in the field of computer use. This criminal possesses skills that qualify them to modify and develop security systems so that no one can track them and follow their criminal activities through networks or inside computer devices (Youssef, 2008, p32)

The cybercriminal is a criminal who relies on intelligence - a person with high technical skills specialized in information crime who exploits their understanding and skills to hack networks and break passwords or codes. They navigate the world of networks to obtain everything valuable and precious from data and information found in computer devices. Through networks, they can use their expertise in hacking and changing information, and

have the ability to modify programs or transfer money. Therefore, we find that most of those who commit these crimes are experts in the field of computers or information technology, and police first search for computer experts when information crimes are committed.

1.2- Classifications of the Cybercriminal

The personality of the cybercriminal, whether natural or legal, and the mechanism of committing the crime make them a person characterized by special features that are added to the other qualities that must be available in an ordinary criminal. (Mohammed Ali Salem, 2008 , p88)

. From what has been presented, some have called these people hackers or crackers. Therefore, we will address the definition of hackers:

a- Definition of Hackers: Called "hacking" in English and "spying," "penetration," or "piracy" in Arabic, where one of the unauthorized persons enters the operating system of a computer illegally and for improper purposes such as spying, theft, or sabotage. The hacker spy is allowed to move, permit, or add files or programs, and can control the operating system by issuing printing, imaging, or sabotage commands: (Al-Tihami, 2008, p03)

These criminals are classified into different categories, including .:

* **Hackers Category - Penetrators or Intruders:** These refer to young adults who are fascinated by information and computers, some of whom are called information prodigies. Most of this category are students and young people with knowledge in the field of information technology. They often adhere to rules of conduct and honor without intending to harm victims. The primary motive for this category is enjoyment and fun by using this technology to prove their skills and abilities to penetrate computer networks through their own effort without assistance from any instructions from other sources, in addition to proving their abilities in discovering and showing weaknesses in information systems without causing harm to them. They may have a desire for adventure, investigation, (Al-Momani, 2003 , p 13) and discovery."

The primary motivations for this group include:

- Enjoying and experimenting with technology
- Proving their skills and abilities
- Independently penetrating computer networks without external instructions
- Discovering and revealing weaknesses in information systems without causing damage
- A desire for adventure, investigation, and discovery (Al-Hamid & Marko Ibrahim, 2007 ,p37)

b- Hackers or professionals:

These work to discover vulnerabilities in order to penetrate systems and applications. This category ranges in age from 25-45 years, and are those who hold high university degrees specializing in computers and information technology. They work as system analysts and programmers and have high awareness of operating programs and deep knowledge of the secrets and vulnerabilities within them. This category is often widespread in America and Europe and has begun to spread in the Arab region as well. (Al-Tihami, 2008, p04).

This category is considered dangerous among technology criminals as they aim to achieve gain for themselves and for the entities that commissioned them - basically to achieve material gain for them or the entities that commissioned and employed them to commit data assault crimes. Some of their attacks also aim to achieve political purposes and express an intellectual, theoretical, or philosophical position. This category is considered more dangerous than the first category, as we can sense good faith in the latter, unlike the second category whose attacks have proven their inclination toward sabotage and crime. (Al-Taif, 2007, p162)

c- The Vengeful Category:

This category is considered the most dangerous of all. Usually, influence and revenge is the prevailing character of their behavior. Members of this category are not characterized by professional technical knowledge, and their activities are technically dominated by the use of viruses and programs to disable the targeted system or site and damage all or some of the data in computer systems, whether from internet sites. .

There are no specific controls regarding their ages, and there are no elements of interaction between members of this category, nor do they boast about their activities but rather seek to hide them. They are the easiest category in terms of discovering the activities they committed due to the availability of circumstances and factors that help with that. On the other hand, this category does not seek to prove their technical and artistic abilities, nor do they seek to achieve material or political gains, nor do they boast or publicize their activities, but work to hide and deny their actions (Hafeez, 2005, p 34)

After studying the classification of criminals who assault data, we decided to study the motives that led to hacking and piracy of data found in computers.

2. Motivations of criminal data abusers:

There is no doubt that human behavior, whatever it may be, has what explains it and what prompted its commission, which is called motives. However, the image of motives is an idea shrouded in some ambiguity and lack of agreement from jurisprudence. Therefore, directions multiplied and differed - some called it the goal, others the intention, others the purpose, and others the motive.

Whatever the case, studying the motives of this type of crime may have a double benefit:

- First, it may help us find appropriate solutions to resist and overcome them
- Second, contributing to determining the legal qualification that may be attributed to them

Therefore, these motives may be personal motives and external motives.

2.1- The first subtitle: Personal Motives

After many studies, scientists and researchers concluded that there are many personal motives that crime perpetrators see as logical reasons to justify their actions and that motivate them to commit such unlawful acts and assaults in cyberspace. Personal motives of the cybercriminal can be attributed to several motives, including financial and mental ones:

a- Financial Motivations:

Seeking to achieve profit ranks first and actually represents the perpetrator's goal and is among the most motivating factors for perpetrators to assault data found in computers. Perpetrators of these crimes with high technical competence, with their experience in the technological field, direct these capabilities toward financial institutions to attempt to achieve financial gains either by stealing those funds or transferring them to their personal account within the bank. Criminals can simply enter bank systems to know computer numbers and steal or transfer them.

Material gain is also a goal for those with less technical knowledge who may be completely unqualified in the information field and cannot access those computer systems. Their method of committing crimes is a specific method in a certain field that does not require experience and skill.

According to studies, the financial sector is the most targeted sector by perpetrators, as these banks rely primarily on electronic financing systems used in the wrong hands. Therefore, millions of dollars can be transferred in seconds to the perpetrator without leaving any evidence against them.

For example, insurance companies are among the sectors targeted by fraud operations, and they sometimes play the role of perpetrator, such as the insurance company (Equitable Funding) in Los Angeles, USA, whose users, with the help of their information system, were able to create fictitious insured clients. This company was able to sell 46 insurance visas to corresponding companies within the framework of reinsurance technical agreements.

The perpetrator, desiring to achieve wealth and material gain, manipulates the automatic processing systems of financial institutions, especially if they are one of its employees, or penetrates their automatic processing systems by discovering their security gaps and works to exploit and program them to transfer financial amounts to their account or their partners'

accounts or the accounts of those for whom they work if they are outside the institution. Financial gains can be obtained through bargaining on programs or information obtained by embezzlement from the computer.

It should be noted that if the criminal succeeds in committing their crime via the internet, this may generate huge profits in record time. We can illustrate the extent of material profits that the criminal achieves as a result of committing this type of crime through what one of these professional criminals in a California prison repeats: "I stole more than half a billion dollars thanks to the tax authority computer devices in the United States of America, and I can repeat that at any time. It was something easy, as I know how the tax computer device works, and I found many loopholes in its system that could provide me with huge amounts if bad luck had not befallen me."

Similarly, what happened in France in 1986, where the return from committing armed robbery was 70,000 French francs, while the fraud crime in the field of automatic information processing yielded 670,000 French francs for the perpetrator..

2.2- : Mental Motives

The mental image of perpetrators of data assault crimes or computer and internet crimes is that of a hero and intelligent person who deserves admiration, not the image of a criminal who should be prosecuted. Perpetrators of these crimes seek to show their superiority and confidence level in their skill to the point that, faced with any emergence of any new technology, perpetrators of these crimes have a passion for the machine and try to find a way to break it or overcome it. Therefore, computer pirates see that obtaining data should not be restricted. The perpetrator dedicates all their effort to learning how to hack prohibited sites. Pirates are often groups whose purpose is cooperation, information exchange, and sharing programs and news. These pirates prefer to remain anonymous so they can continue to exist for the longest possible period, while interest in computer security increases through developing new and difficult ways to hack it, such as encryption software that only its recipient can understand.

For example, the US Department of Defense (Pentagon) changes the data encoding systems used daily, so that some sensitive information changes its encoding systems every hour. This undoubtedly indicates a high degree of technology and system. Therefore, we see electronic enthusiasts competing to breach these systems and show their superiority over them. Evidence of this is when an amateur in Europe solved the code of one of the Pentagon information centers and was able to tamper with this center's data.

Some have argued that the motives for committing data assault crimes may be the desire to challenge and defeat the system and overcome the complexity of technological means.

Penetrating electronic systems and breaking the security barriers surrounding these systems may constitute great pleasure for the perpetrator and entertainment that covers their leisure time, as the criminal here tends to show their superiority over technological means and considers this among the motives of challenge and proving capability.

2-3: External Motives

To commit some data assault crimes, humans are influenced by external influences as a result of their existence in the automatic data processing or information environment. The influences that push individuals to commit such behavior are considered, whether political motives or revenge motives.

a- Political motives:

Political motives are among the most prominent motivations for international attempts to hack government networks in various countries of the world. Individuals may also be able to hack government security devices. Therefore, the internet has become a fertile field for spreading the ideas of many individuals and communities and a means for promoting news and other matters that may carry harm to state security or the system of government or international symbols and offend them through slander and defamation.

Many undesirable sites have spread on the internet for several motives, including those directed against a specific state's policy or against a particular belief or doctrine. They primarily aim to distort the image of the targeted state or belief. In hostile political sites, news and information are often fabricated, even falsely, or even based on a very small part of the truth and then weaving fabricated news around it. (Al-Mushair, 2009, p39)

Many undesirable sites have spread on the Internet for several motives, and among these motives are those that are directed against the policy of a specific country or against a specific doctrine or belief, and they aim primarily to distort the image of the targeted country or belief, and often in hostile political sites, news and information are fabricated, even if falsely or even based on a very small part of the truth and then weave fabricated news around it. The owners of these sites often create a database of people's addresses that they obtain from companies that follow these databases, or in other ways, and then add those addresses to their mailing list and start flooding those addresses with their publications, and they usually resort to this method in order to bypass the blocking that they may be exposed to and to communicate their voices as much as possible. (Al-Momani, 2003 , p45)

b- Revenge as a Motive

Revenge is one of the most dangerous motives that can drive an individual to commit a crime. This is especially true in the context of cybercrime, where the perpetrator often possesses extensive knowledge about the organization or company they work for. This motive

is usually rooted in professional grievances, such as feeling deprived of certain professional rights or being unfairly dismissed from their job. This sense of injustice can fuel a desire for revenge against the employer.

Many individuals are unjustly terminated from companies or government organizations. Armed with the necessary information, training, and knowledge of the organization's inner workings, these former employees are often driven to commit cybercrimes." (Al-Shawa, 2003 , p32)

b- The Motive of Causing Harm to Individuals or Specific Entities:

Some crimes committed via the internet have the motive of harming specific persons or entities. These crimes are often direct, committed in the form of blackmail, threats, or defamation, such as what happened in Dubai, United Arab Emirates, when someone pirated girls' photos and raided the email of a group of girls in that country, stealing their personal photos and publishing them on an internet site with a group of pornographic photos.

Also, what happened in Saudi Arabia when someone hacked the email of a girl in Saudi Arabia, obtained some of her personal photos, and later blackmailed her. They may be indirect, consisting of obtaining data and information about those entities or persons for later use in committing direct crimes

d -Commercial and Economic Motivations

The internet has opened up entirely new avenues for commerce, allowing businesses to operate rapidly without the need for costly traditional communication channels. It has provided equal opportunities for everyone around the world, imposed economic limits, and offered security in information exchange within and between organizations that are geographically distant from each other, thereby expanding the customer base. Additionally, the network's mobility has facilitated the exploration of new forms of services and goods. For example, the internet enables users to make reservations worldwide, including booking tickets for sporting events, entertainment activities, and travel by air, sea, and rail. A successful system for pre-booking railway tickets for travel on the lines of the Commonwealth of Independent States countries is currently operating in Russia. The emergence of online marketing has provided new, inexpensive, fast, and efficient opportunities. Web pages can be updated within seconds, and some argue that the faster information reaches customers, the quicker they are to make a purchasing decision. (mohmed, 2016)

Conclusion:

" At the conclusion of this research paper, we conclude that information crime requires high technical expertise that is difficult for traditional investigators to deal with. Given what

these crimes require in terms of technology to commit them, they require high competencies to discover and investigate them. Therefore, judicial police officers find themselves unable to deal with investigative means and traditional procedures with this type of crime, in addition to the difficulty of conducting secret investigations and tracking cross-border electronic operations.

Police officers may not deal skillfully and professionally with electronic evidence derived from the crime, and if found, they may unintentionally damage it. Therefore, we suggest the following:

- Joint training courses must be held between judiciary members from the Public Prosecution and police officers and technical experts together, for the purpose of knowing the largest possible amount of information about hacking and piracy of information and data, etc., so that the most appropriate legal methods are reached to combat this type of crime while enhancing cooperation between national and international judicial authorities.
- Allocating centers by computer experts to train police personnel to confront cybercriminals and holding continuous training sessions that keep pace with the development of information crime in general and cybercriminals in particular.
- Exploiting scientific competencies and providing reasons, especially economic ones, so as not to turn this category into a tool of destruction in society.

List of references:

- Al-Hamid, M., & Marko Ibrahim, N. (2007). *Protection of Information Systems* (éd. 1st Edition). Amman: Dar Hamed for Publishing and Distribution.
- Al-Momani, A. (2003). Penal Law in Confronting Internet Risks. *Master's Thesis in Criminal Law*, 13., Annaba University, , Algeria.
- Al-Mushair, T. b. (2009). , Building a security model to combat cybercrime and measuring its effectiveness. *PhD thesis* . Riyadh , Faculty of Graduate Studies ,Naif Arab University for Security Sciences.
- Al-Shawa, M. S. (2003). *The Information Revolution and its Implications on the Penal Code*. Arab Renaissance House.
- Al-Taif, J. (2007). *Information Technology Crimes*. Amman: Dar Al-Bidaya.
- Al-Tihami, Y. R. (2008). *"Hacker Tricks"* .
- Hafeez, A. A. (2005). *Technical and security trends to confront cybercrime*.
- Hijazi, A. F. (2008). , *Forgery in Computer and Internet Crimes*. Egypt: , Dar Al-Kutub Al-Qanuniya.
- Mohammed Ali Salem, H. O. (2008). The Noise of Cyber Crime. *Babylon University Journal* .
- mohmed. (2016, 06 04). *www.diae.net accessed* . Consulté le 08 16, 2025
- Youssef, A. F. (2008). *Cyber Crimes on the Internet*,. Alexandria: University Publications House.