

Sociological analysis of cybercrime in Algerian society

TERCHOUNE Hana*

Laboratory Development, deviance and crime in society, university of
Badji Mokhtar -Annaba-, (Algeria),
E-Mail: hana.terchoune@univ-annaba.dz

Submitted

10/10/2025

Accepted

22/04/2026

Published

01/06/2026

Abstract: This study aims to analyze the phenomenon of cybercrime in the Algerian digital space from a sociological perspective, seeking to understand the social, economic, and cultural factors that contribute to its formation and spread. The paper does not treat cybercrime as merely a technical act, but as an outcome of a complex social context where the individual interacts with their environment. The methodology relies on the secondary analysis of official statistics from the National Office for the Fight against Cybercrime (ONLCC) and the Postal and Telecommunications Regulatory Authority (ARPT), coupled with a critical review of explanatory sociological theories of deviance, such as Merton's Strain Theory and Sutherland's Differential Association Theory.

Keywords: *Cybercrime, Sociology, Algerian Society, Social Analysis, Digital Divide.*

Introduction:

Cybercrime is one of the most significant challenges facing contemporary societies in the era of digital transformation. It has gone beyond being merely a technical violation to become a complex social phenomenon that reflects profound imbalances in the structure and values of society (Yar.M,2006, P4). In the Algerian context, this phenomenon is of particular importance given the rapid transformation that society is undergoing in terms of the spread of internet and social media use, coupled with a young demographic and profound socio-economic changes (Bouznina,2021, P45).

The rapid adoption of digital technologies in Algeria, which has not always been accompanied by a similar development in security awareness or an effective legislative framework, has opened up new avenues for deviant behaviour. Cyberspace is no longer just a communication tool, but has become a new arena for social and economic conflict, where new forms of crime such as financial

* Corresponding author

fraud, cyber extortion and identity theft are emerging, reflecting the frustrations and aspirations of certain social groups, especially young people(ONLCC,2022, P8).

This is the starting point for this article, which focuses on the main question:

How do sociological factors and variables contribute to the formation and spread of cybercrime in Algerian society?

This question gives rise to several sub-questions:

- 1- What are the socio-demographic characteristics of perpetrators and victims? Which sociological theories can provide a convincing explanation for this phenomenon?
- 2- What is the role of the Algerian social context (economic, cultural, educational) in fuelling it?

- Objectives of the study:

This study aims to provide an in-depth sociological analysis of cybercrime in Algeria, seeking to explain it beyond the narrow technical-security approach. It also aims to link recent official statistical data with sociological theoretical frameworks in order to produce a proactive reading that contributes to the development of effective prevention and treatment policies.

- Study methodology:

The study methodology is based on a secondary analysis of quantitative and qualitative data available in official reports from the National Office for the Fight against Cybercrime (ONLCC) and the National Regulatory Authority for Post and Telecommunications (ARPT). It will also draw on an interpretive sociological approach, using a set of classical and contemporary theories in the sociology of deviance and crime to understand the non-technical dimensions of the phenomenon.

The study will be organised in a sequential manner, beginning with the framing of concepts and theories, followed by the presentation and analysis of official statistics in their social context, then moving on to the analysis of explanatory sociological factors (economic, cultural, socio-psychological), and concluding with the drawing of conclusions and the presentation of recommendations based on social analysis.

1-Theoretical and Conceptual Framework:

To understand the complex phenomenon of cybercrime in its social dimension, one cannot rely solely on technical or legal approaches. It is necessary to draw on

a theoretical framework capable of explaining deviant behaviour in its social context. The sociology of deviance and crime provides an ideal framework for this purpose, as it examines the social, cultural and structural factors that drive individuals towards socially unacceptable behaviour, including in cyberspace (Jaishankar, 2011, P12).

1-1- Basic concepts of the study:

A- Cybercrime: The study defines it not merely as an act that violates the law, but as a socio-technical phenomenon that includes any criminal activity that uses the digital network as a tool or target, and results from the interaction between individual or collective motives and technical capabilities in a specific social context that encourages or allows such behaviour (Furnell, 2002, P5)

B- Cybersecurity Awareness: This refers to an individual's degree of awareness of the risks and threats in the digital space and their knowledge of safe practices to protect themselves and their information assets. The absence of this awareness is one of the important social factors that fuel crime.

C- Digital Divide: This is not limited to the gap in access to technology between the rich and the poor, but also includes the gap in skills and safe use between generations (young and old) and between geographical areas (urban and rural). This divide creates a fertile environment for exploitation and victimisation (Van Dijk, 2020, P3).

D- Virtual Community: Refers to groups of individuals who interact primarily online. These communities play a crucial role in shaping values and behaviours, including deviant ones, according to differential association theory.

1-2- Explanatory sociological theories:

A- Strain Theory - Robert K. Merton:

This theory is one of the most appropriate for explaining cybercrime in the Algerian context. Merton believes that crime arises when there is a gap between the cultural goals promoted by society (such as material wealth and success) and the legitimate means available to individuals to achieve these goals (Merton, 1938, P672). In Algeria, where finding stable employment and housing is a major challenge for young people, the frustration caused by this gap may lead some individuals to view cyberspace as an alternative arena for achieving quick 'success' through illicit means, such as cyber fraud or hacking.

B- Differential Association Theory – Edwin H. Sutherland:

This theory assumes that criminal behaviour is learned rather than innate, and is learned through interaction with others in primary groups. In the digital world (Sutherland, 1947,P6), this ‘learning’ takes place intensively through secret hacking forums, Telegram channels, and social media groups, where hacking techniques and values and narratives justifying criminal behaviour are transmitted. This explains the prevalence of crimes such as identity theft and malware development.

C- Pierre Bourdieu's concepts:

The concepts of cultural capital and social capital can be used to understand the gap in dealing with the digital space. Weak digital cultural capital (security knowledge and skills) increases an individual's vulnerability to becoming a victim. Conversely, perpetrators can exploit their technical skills (as a form of cultural capital) to compensate for a lack of economic or social capital in the real world (Bourdieu, 1986, P 241).

2- The Socio-Technological Context in Algeria

Understanding the environment in which cybercrime thrives is crucial to deciphering its social codes. Algeria's rapid digital transformation, coupled with unique demographic and social characteristics, has created fertile ground for the emergence and development of new forms of deviance.

2-1- The spread of the internet and mobile phones:

Over the past decade, Algeria has witnessed a quantum leap in the penetration of internet services, driven mainly by the shift towards modern technologies such as 3G, 4G and 5G, and the spread of affordable smartphones (ARPT, 2023, P15). The following table shows this rapid development, which has outpaced the development of traditional social infrastructure.

Year	Number of Broadband Internet Subscribers (in millions)	Penetration Rate (%) of Total Population
2015	7,50	18,90%
2018	12,10	29,50%
2021	18,30	41,20%
2023	22,50	49,80%

Evolution of the number of Internet subscribers in Algeria (2015-2023) based on data from the National Telecommunications Regulatory Authority (ARPT)

- Sociological analysis of the table:

The table shows a significant acceleration in internet connectivity, with penetration jumping from less than 20% to nearly 50% in less than a decade. This acceleration means that new and broader social segments (less educated, less security-aware, older age groups or rural areas) are suddenly entering the digital space. This ‘digital shock’ widens the gap between technical ability to use the internet and social ability to use it safely, increasing victimisation rates and creating opportunities for perpetrators to exploit this vulnerability (Doudi, 2022, P89).

2-2- Demographic characteristics: a young society

Algeria is a very ‘young’ country, with people under the age of 30 making up a large proportion of the total population (ONS, 2022). This group is the most active and adaptable when it comes to digital technologies, but it is also the most vulnerable to unemployment and frustration. Consequently, the virtual space becomes a dual space for young Algerians: a place for entertainment and socialising, and a potential space for seeking economic opportunities (legitimate or otherwise) in response to the difficulty of integrating into the traditional labour market.

2-3- Changes in patterns of communication and expression of identity:

Social media has profoundly changed the nature of social interaction. These platforms have become the primary space for the construction of individual and collective identity, especially for young people (Boukhalfa, 2021, P115). This shift has been accompanied by a weakening of traditional family and community control, with individuals enjoying greater freedom that may extend beyond the norms and values prevailing in the real world, facilitating behaviours that would have been difficult to carry out in public.

3- Legal and institutional framework for combating cybercrime

Legal and institutional frameworks represent the formal structure through which the state deals with the phenomenon of cybercrime. In Algeria, this framework is undergoing continuous development in an attempt to keep pace with the increasing complexity of these crimes, but it still faces a number of practical challenges.

3-1- Legal framework: Law on Combating Cybercrime (Law 09-04)

Law 09-04 of 5 August 2009, as amended and supplemented, is the backbone of Algerian legislation in this area (JO, 2009, P14). This law aims to 'suppress crimes related to automated data processing systems' and seeks to define criminal acts in cyberspace and establish appropriate penalties for them. Among the most notable crimes it addresses are:

- **Crimes against automated processing systems:** such as illegal access to the system, obstruction of its operation, fraudulent entry or deletion of data.
- **Crimes committed by these systems:** such as electronic fraud, forgery, and infringement of individual freedoms (blackmail, invasion of privacy).
- **Content crimes:** such as the dissemination of pornographic or child abuse material and hate speech.

However, critics argue that, more than a decade after its enactment, the law suffers from certain loopholes in light of technological developments, and that some penalties may not be sufficiently dissuasive given the seriousness of certain acts (Benhamouda, 2020, P45).

3-2- Institutional framework: National Office for the Fight against Cybercrime (ONLCC):

The National Office for the Fight against Cybercrime was established by Executive Decree 11-09 of 3 January 2011 and is under the authority of the Directorate General of National Security (ED, 2011). This specialised structure is responsible for the following tasks:

- **Combating cybercrime:** investigating and prosecuting crimes against information systems.
- **Victim support:** receiving complaints from affected citizens and institutions.
- **Prevention and awareness:** promoting a culture of security among internet users.
- **International cooperation:** exchanging information and expertise with similar agencies in other countries.

The creation of the ONLCC represents official recognition of the specific nature of cybercrime and the need for a specialised agency to combat it. Its annual reports show a marked increase in the number of cases recorded, reflecting both the growth of the phenomenon and the development of the agency's monitoring and tracking capabilities (ONLCC, 2022, P5).

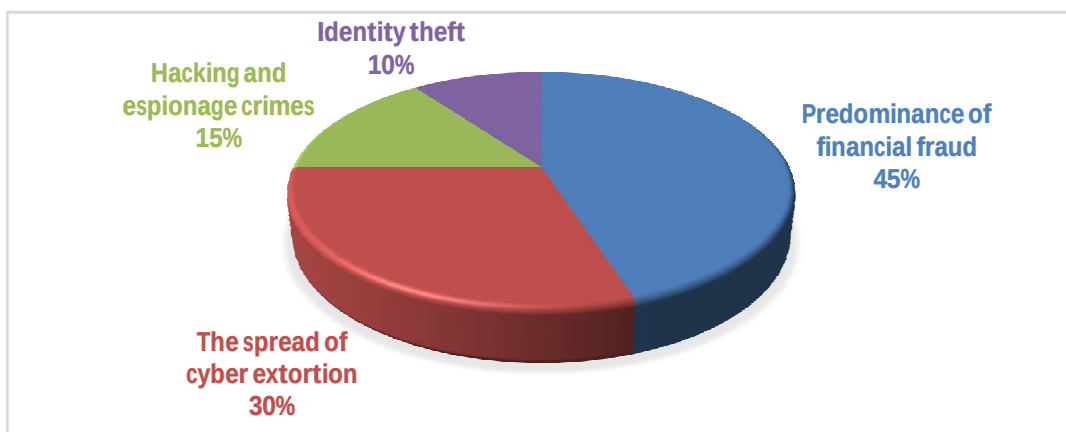
3-3- Implementation issues and challenges:

Despite the existence of this framework, the fight against cybercrime continues to face considerable challenges, most notably:

- **The rapid pace of technological development:** Criminals' methods evolve at a pace that often exceeds the speed at which laws are updated and the capabilities of security agencies are strengthened.
- **Difficulty of tracking and globalisation:** The cross-border nature of cybercrime makes it difficult to track perpetrators, who may be operating from outside the national territory, requiring international judicial and security cooperation, which is not always easy (Benabdallah, 2021).
- **Lack of specialised human resources:** The need for highly skilled technical and legal personnel remains an obstacle in some cases.

4- Official Cybercrime Statistics: A Typological Analysis

Official statistics published by the National Office for the Fight against Cybercrime (ONLCC) represent the most objective quantitative indicator for measuring the scale and nature of the phenomenon in Algeria. Analysing this data from a qualitative perspective provides an understanding of the prevailing criminal priorities and shifts in criminal behaviour, which forms the basis for applying interpretative sociological approaches (ONLCC, 2023, P8). These statistics only reflect crimes that have been reported and recorded by the security services, which means that the real figure may be higher (the 'dark figure' phenomenon).



Distribution of cybercrimes recorded in Algeria by type Data inspired by ONLCC reports for the year 2023

- Sociological analysis of the main types of crimes:

A- Predominance of financial fraud (45%):

This strikingly high percentage reflects the priority of direct economic motivation among perpetrators. From a sociological perspective, this can be explained through the lens of social disorganisation theory (Merton). In a social context marked by high youth unemployment (particularly among university graduates) and economic pressures, cyberspace appears to be a 'lucrative' and quick arena for making money through illegal means (Merton, 1938, P682). Only moderate technical skills are required to carry out fraud through fake sales platforms or phishing, making it a 'rational' choice from the perspective of a potential criminal who sees limited opportunities in the formal economy.

B- The spread of cyber extortion (30%):

These crimes represent a clear psychosocial dimension. They often exploit gaps in individuals' social behaviour (such as sharing private content online) rather than technical vulnerabilities. Here, differential association theory (Sutherland) comes into play to explain how perpetrators learn psychological blackmail techniques and manipulation methods through communication in dark web communities or closed groups (Sutherland, 1947, P6). These crimes also reflect a crisis of values linked to the decline of moral restraint in virtual space, where perpetrators feel a degree of impunity due to anonymity.

C- Hacking and espionage crimes (15%):

These crimes are often associated with actors who have high technical skills (technical cultural capital). Their motives may be economic (selling stolen data) or even 'personal,' such as self-affirmation and seeking recognition among their peers in hacker communities (Breton, 2000, P78). This is consistent with Pierre Bourdieu's interpretation, whereby individuals use their cultural capital (technical knowledge) to gain status or benefits in a particular social field (cyberspace), even if this is outside the bounds of what is considered legitimate.

D- Identity theft (10%):

These crimes reflect a desire to obtain indirect benefits, whether social (defaming others, damaging their reputation) or financial (accessing bank accounts). From a social perspective, they point to an identity crisis and how digital identity is used as a tool for harm in the context of personal conflicts or social competition (Al-'Ifa, 2021, P120).

5- Socio-Demographic Profile of Offenders

Analysing the socio-demographic characteristics of individuals involved in cybercrime is essential to understanding the social mechanisms that produce criminal behaviour. Although it is difficult to obtain accurate and comprehensive data on the characteristics of perpetrators due to the nature of these crimes, official reports and field studies allow us to draw a general picture that shows a clear concentration in specific social groups (Furnell, 2002, P124).

Age Group	Approximate Percentage (%)
Under 20 years	15%
20 – 30 years	55%
31 – 40 years	20%
Over 40 years	10%

Proportional distribution of suspects in cybercrime cases by age group (data inspired by ONLCC reports)

-Sociological analysis of data:

A- The adolescent category (under 20 years old, 15%):

The motives of individuals in this category are often not entirely economic. They may be motivated by a desire to prove their technical skills, curiosity, or peer pressure. Here, Sutherland's differential association theory finds its application, where the values and behaviours of hacking are learned through mixing with online groups that encourage and justify such actions.

Weak moral restraint and a desire for self-affirmation make this group susceptible to deviant behaviour.

B- The absolute dominance of young people (20-30 years old, 55%):

This concentration indicates a strong relationship between the stage of 'youthful maturity' and involvement in cybercriminal behaviour. This period is the peak of the search for economic and social independence and identity formation. In the Algerian context, where this group suffers from high unemployment rates and delayed marriage and independence, this creates a state of 'anomie, a condition described by Durkheim in which social norms become unclear or ineffective (Dubet, 2010, P89). This frustration drives young people to seek alternatives, and they may find in cyberspace a way to compensate for their failure in the real world, either in pursuit of financial gain (fraud) or in search of recognition and appreciation (hacking).

C- Age group (31-40 years old, 20%):

The 20% represented by the 31-40 age group is a clear warning sign of the evolution and centralisation of cyber threats. It reflects not only the continuation of criminal behaviour by some individuals as they age, but also the entry of new individuals into this path, driven by economic crises and severe life pressures, but using more sophisticated and dangerous tools. This calls for the development of countermeasures that focus on internal monitoring within organisations and raising awareness among employees in mid-career about the risks of drifting into crime.

D- Decline in the phenomenon with age (10% over 40 years old):

This decline reflects several factors: social and economic stability, maturity of character and clarity of moral standards, as well as a digital skills gap, with older people being less adept at using the complex technologies required to commit many cybercrimes.

F- Other characteristics: Educational level and economic status:

Most cases indicate that those involved often have a medium to high level of education, especially in technical fields (informatics, electronics) (Belaroussi, 2022,P55). This point is extremely important, as it shows that cybercrime is not the result of ignorance, but is often the result of the use of legitimate knowledge for illegitimate purposes.

These individuals possess technical cultural capital but lack economic capital or social capital (networks of relationships that open doors to employment), prompting them to 'invest' their skills in the black market of the internet (Bourdieu, 1986, P241). This phenomenon reaffirms the relevance of Mertonian theory on the gap between means (technical knowledge) and ends (material success).

6- Explanatory Sociological Factors:

6-1- Economic Dimension and Deprivation

The economic dimension is the cornerstone of any sociological analysis of crime, including cybercrime. Direct material motives are among the strongest drivers of criminal behaviour, especially in a social context where there is a widening gap between legitimate aspirations and the means available to achieve them. In Algeria, the general economic context, characterised mainly by high unemployment rates and deteriorating living conditions for a large segment of

young people, provides fertile ground for justifying and encouraging involvement in illegal online activities (Agnew, 1992, P47).

-Unemployment as a key stress factor:

Data from the National Statistics Office (ONS) indicate that the unemployment rate among young people (under 30) remains alarmingly high, exceeding 25% (ONS, 2023). This abstract figure translates into a daily reality of frustration, despair and uncertainty about the future. In such an environment, many young people lose faith in the usefulness of legitimate pathways (education, vocational training)

As a means of achieving social and economic integration. According to Strain Theory, this pressure drives individuals to seek alternative, non-traditional ways of achieving the material and social goals that they are unable to attain through legitimate means (Merton, 1938, P672). Cyberspace, far from the watchful eye of the authorities, offers them this 'alternative means' that appears less costly and risky than traditional crime.

- Cybercrime as a 'rational process':

From an economic-sociological perspective, the decision to engage in cybercrime can be seen as a somewhat 'rational' decision by the perpetrator, based on an implicit process of cost-benefit analysis (Lagrange, 2010). On the one hand, the expected cost is relatively low: the chances of catching the perpetrator are slim compared to physical crimes (due to the difficulty of tracking and concealment), and legal penalties, although they exist, may not be sufficiently deterrent in the eyes of the potential perpetrator. On the other hand, the expected return is high: quick financial gains from fraud, or achieving 'fame' and recognition in hacker communities. When the balance of this equation favours the return, especially in the absence of real opportunities for legitimate returns, deviance becomes an attractive option.

- Consumption patterns and the pressure to 'get rich quick':

In an increasingly commodified society where consumerism and get-rich-quick culture are promoted through the media and social media, there is growing pressure on individuals, especially young people, to strive for this lifestyle (Ben Omar, 2021, P210). This creates an additional gap between the modest reality of many people's lives and the idealised image that is promoted. Cybercrime, especially financial fraud, offers the promise of quickly narrowing this gap. In other words, crime is committed not only to meet basic needs, but also to satisfy imported 'needs' created by socialisation in a globalised consumer culture.

The analysis shows that the economic factor is not merely a circumstantial motive, but a deep structural factor that interacts with social and cultural structures. Relative deprivation – the feeling of deprivation compared to others or to the ideal image – is what generates frustration and anger that can fuel criminal behaviour. Therefore, any cybercrime prevention policy must take into account addressing these economic roots by creating real opportunities for young people and restoring confidence in legitimate paths to success.

6-2- Cultural and Educational Dimension

In parallel with economic factors, the cultural and educational dimension plays a decisive role in shaping individual and collective behaviour towards the digital space. Weak digital education and the moral ambiguity accompanying the rapid shift towards digitalisation contribute to creating an environment that increases an individual's vulnerability to becoming a victim or perpetrator. This dimension is evident in the failure of traditional social institutions to keep pace with the technological revolution and provide individuals with the cultural and ethical tools necessary to deal with it safely (Livingstone& Haddon, 2009).

* Failure of social institutions: family and school:

- **The digital divide between generations within the family:** Many Algerian families find themselves unable to monitor and guide their children's use of the internet. Children are often more tech-savvy than their parents, causing parents to lose their traditional role as guides and transmitters of norms(MNE, 2022). This 'knowledge inequality' reflects what Pierre Bourdieu called the difference in cultural capital between generations. This lack of effective parental supervision leaves young people and adolescents face to face with digital content that may be harmful and, in some cases, with the temptation to engage in dangerous behaviour without any direct moral deterrent.
- **The shortcomings of Algerian schools:** The education system in Algeria has continued to focus on traditional education, introducing digital citizenship and safe internet use in a marginal and unsystematic manner (Hachani,2020,P330). Schools, which are supposed to be a lever for modernisation, have not yet been able to produce 'digital citizens' armed with knowledge, critical thinking and ethics. This failure leaves a large segment of young people without cultural immunity against the dangers of cyberspace.

*** The crisis of values and the spread of the ‘get rich quick’ culture:**

Algerian society, like other societies, is witnessing a clash of values between tradition and collective solidarity on the one hand, and individualism, consumerism and rapid material success promoted by globalisation and digital spaces on the other□. In this conflict, traditional moral values (honesty, respect, integrity) may be declining in favour of values of immediate individual benefit. Social media platforms promote models of rapid and unconventional ‘success’, reinforcing a culture of ‘get rich quick’ and diminishing the value of hard work and honest labour. This cultural environment weakens internal moral restraint and makes individuals more receptive to the idea of using any means, including illegal ones, to achieve success and recognition.

*** Weak cyber-security awareness:**

The low level of security awareness among internet users in Algeria is one of the key cultural factors. This is evident in simple but dangerous practices, such as (ENISA, 2022):

- Using weak passwords.
- Sharing personal information insecurely.
- Clicking on suspicious links.
- Overconfidence in online transactions.

This vulnerability is not limited to the general public, but may also extend to some technical professionals who may have the skills but lack ‘security culture.’ This makes the entire society an environment rich in potential victims, encouraging criminals to continue their activities due to the ease of achieving their goals.

The intersection of failed socialisation, a crisis of values, and weak security awareness creates a perfect ‘cultural storm’ that fuels cybercrime. Addressing this dimension requires a genuine cultural and educational revolution, starting with reforming the education system to teach digital citizenship, launching large-scale awareness campaigns targeting all age groups, and reproducing a cultural discourse that combines authenticity and moral values on the one hand, and the requirements of the digital age on the other.

6-3- Psycho-Social Dimension and Identity:

After analysing the economic and cultural dimensions, it remains necessary to delve into the socio-psychological depth of the actors, where individual psychological needs interact with social dynamics in the virtual space. Cybercrime is not only about seeking material gain, but can also be a means of satisfying deep

psychological needs such as recognition, self-affirmation and the search for identity, especially in a social context where many young people feel excluded and alienated from the real world (Suler, 2004, P321).

*** Virtual space as a refuge for identity and recognition:**

For a young Algerian who may feel socially or economically marginalised, cyberspace becomes a 'refuge' and an alternative space for building identity and gaining recognition that he may be unable to achieve in his immediate environment(Aubert, 2010). By mastering complex technical skills (such as hacking systems), individuals can build a powerful and respected new identity for themselves within hacker communities or on social media platforms. This 'compensatory' identity gives them a sense of power, control and recognition that they lack in their daily lives. Therefore, the motives of some perpetrators may be non-material in nature, but rather a symbolic quest to compensate for feelings of inferiority or helplessness in the real world.

*** The influence of peer groups and differential association online:**

Sunderland's theory emphasises that deviance is a behaviour learned through intimate communication within primary groups (Sutherland, 1947, P6). In the digital age, these groups are no longer limited to the neighbourhood or school, but have expanded to include 'virtual peer groups' in chat rooms, hacking forums, and secret channels on applications such as Telegram and Discord. Within these groups, technical knowledge of criminality is exchanged, but more importantly, values, attitudes, and techniques of moral neutrality that justify criminal behaviour are transmitted (e.g., 'everyone does it,' 'big companies are rich and don't deserve pity, 'it's just a test of skill'). Individuals find support and social justification for their deviant behaviour within these groups, which weakens their internal social control barriers.

*** The feeling of impunity and the absence of effective oversight (The Online Disinhibition Effect):**

Cyberspace creates what is known in psychology as the 'online disinhibition effect'. This effect is the result of several factors:

- **Anonymity:** Users feel invisible, which reduces their fear of social or legal punishment.
- **Invisibility:** The absence of body language and immediate reactions makes it easier to harm or deceive others.
- **Asynchronicity:** The lack of immediate interaction reduces the sense of direct responsibility for one's actions.

These factors combined weaken an individual's 'social conscience' and make them more daring to commit acts that they would not commit face to face. In the

Algerian context, where the culture of 'shame' (in the real world) remains a powerful social deterrent, the virtual space provides an outlet for liberation from these pressures, but this disintegration can reach the level of criminal behaviour.

*** Symbolic violence and social conflict:**

Some crimes, such as cyberbullying or hacking into specific people's accounts, can be interpreted as a form of Forms of symbolic violence practised in the context of hidden social conflicts (Bouakkaz, 2023, P145). Crime may be a means of revenge against an adversary, of settling scores, or of bringing down a social symbol (such as a public figure) as a way of venting collective frustration. In this case, cybercrime is merely a modern tool for traditional social conflicts.

This dimension shows that psychological and social motives are intricately intertwined. Cybercrime may, in many cases, be a symptom of a deeper social malaise related to identity crisis, alienation, and the search for recognition in a rapidly changing society. Therefore, a purely security-based approach is incapable of addressing these root causes, necessitating the integration of psychological and social support and reintegration mechanisms into crime prevention policies.

7- Sociological Analysis of Victims:

A sociological analysis of cybercrime is incomplete without focusing on the other side of the equation: the victims. Studying the characteristics of victims and the social factors that increase their vulnerability to victimisation is no less important than studying the perpetrators. This study does not aim to blame the victim, but rather to understand the social dynamics that make certain individuals or groups more vulnerable than others, thereby opening the door to the development of targeted and effective prevention strategies (Walklate, 2007, P5)

Social groups most vulnerable to cybercrime (based on analysis of crime patterns in official reports)

Sociological Factors Explaining Vulnerability	Most Common Types of Cybercrimes	Social Group
Digital skills gap: Weak technical knowledge makes them less capable of recognizing phishing attempts. Excessive trust: Social upbringing that reinforces trust in others may not align with the deceptive nature of the virtual world. Social isolation: The search for connection through the internet can increase susceptibility to emotional and financial exploitation.	Financial fraud (fake donations, credit card scams), identity theft.	Elderly (50+)
Gender-based social profiling: Women are targeted as a “weak link” in a patriarchal society that may hesitate to support the victim for fear of “scandal.” Social control over behavior: The threat of publishing private (real or fabricated) content becomes an effective blackmail tool. Nature of social interaction: Social pressures may push women to seek relationships online, increasing their vulnerability points.	Sexual and cyber blackmail, cyberstalking, identity theft, defamation.	Women and young females
Curiosity and inexperience: Make them easy targets for criminals. Need for social acceptance: The desire to make friends or gain popularity on platforms may lead them to share personal information or engage in risky behavior. Lack of effective parental supervision: Due to the generational monitoring gap mentioned earlier.	Online sexual exploitation, cyberbullying, online gaming fraud.	Children and adolescents
Desire for quick profit: Coupled with limited resources dedicated to cybersecurity compared to large companies. Increasing reliance on online marketing: Without sufficient security awareness to protect themselves. Weak security infrastructure: Found in many small institutions.	Commercial fraud (via sales platforms), extortion, system hacking for data theft.	Small business owners and traders

- **Identifying vulnerable groups (perpetrators and victims):** The analysis highlighted that both perpetrators and victims belong to specific vulnerable social groups. Perpetrators are concentrated among unemployed and frustrated young people, while victims are more likely to be elderly people, women, children, and small business owners—those who are less fortunate in terms of digital cultural capital and less protected by the social structure.

- **Failure of socialisation institutions:** The analysis revealed a clear shortcoming in the performance of Algerian families and schools in preparing ‘digital citizens’

equipped with knowledge and ethics. This educational gap has left individuals face to face with the dangers of the digital space without adequate tools for protection.

- **Shortcomings of the current security-legal approach:** The study showed that the current approach (Cohen& Felson,1979, P588), despite its importance, suffers from shortcomings in addressing the root causes of the phenomenon because it does not deal with the social roots of crime, such as unemployment, the crisis of values, and the weakness of digital education.

*** Emphasis on the central issue:**

It can be asserted that sociological factors and variables (economic, cultural, psychological and social) play a decisive and crucial role in the formation and spread of cybercrime in Algerian society. They are not merely a backdrop, but rather effective drivers that create incentives, weaken deterrents, and create an environment conducive to the proliferation of deviant behaviour.

8- Suggestions and recommendations:

A comprehensive sociological analysis of cybercrime in Algerian society has yielded a set of insights that allow for the formulation of practical recommendations based on the findings themselves. These recommendations aim to address the social roots of the phenomenon, not just its symptoms, through a multi-level approach that includes educational, economic, legal and institutional aspects.

A- Sociological and educational recommendations (addressing the roots):

-Integrating digital education and cybersecurity into educational curricula:

The Ministry of National Education should make 'digital citizenship education' a compulsory and systematic subject at all levels of education, from primary to secondary school. This subject should focus on promoting security awareness, digital ethics, combating hate speech, and how to detect fraud.

- **Organising large-scale, targeted awareness campaigns:** Developing awareness programmes tailored to the most vulnerable groups, such as:

- Simplified programmes for older people, in collaboration with civil society organisations, focusing on the basics of fraud protection.
- Awareness campaigns for women on how to deal with cyber extortion and reporting mechanisms.
- Workshops for small business owners on securing their online activities.

***Strengthening the role of the family:** Developing support and guidance programmes for parents to enable them to understand digital risks and effectively monitor their children's activities, thereby bridging the digital generation gap.

B- Economic and social recommendations (addressing incentives):

*** Creating real opportunities for the economic integration of young people:**

Reducing youth unemployment, especially among graduates in technical fields, must be at the heart of economic policy. This can be achieved by:

- Encouraging entrepreneurship in the legitimate digital sphere (e.g. app development, e-marketing) through incubator funding and soft loans.
- Directing investment towards sectors that generate employment opportunities for young people.

***Developing the national digital economy:** Creating an environment that encourages the legitimate digital economy provides an attractive alternative to the informal and criminal economy and channels young people's energies towards producing real value.

C- Legal and institutional recommendations (strengthening frameworks):

*** Review and update Law 09-04:** Review the law on combating cybercrime to keep pace with developments, focusing on:

- Tightening penalties for extortion and hacking offences to make them more dissuasive.
- Including clear provisions for the protection of personal data in line with the European model (GDPR).

*** Strengthening the capacities of the National Office for the Fight against Cybercrime (ONLCC): Supporting the ONLCC by:**

- Providing it with greater human and technical resources.
- Developing its capabilities in the field of advanced and proactive digital investigations.
- Strengthening international cooperation with similar agencies, particularly with neighbouring Maghreb countries.

*** Establishing a national cybercrime observatory:** Its mission is to systematically collect and analyse data, conduct in-depth sociological studies to understand shifts in crime patterns, and provide informed recommendations to decision-makers.

D- Recommendations related to scientific research:

*** Encourage sociological scientific research in the field of cybercrime:** Urge universities and research centres to conduct in-depth field studies on the socio-demographic characteristics of perpetrators and victims, motives for crime, and the effectiveness of countermeasures, in order to inform public policy with accurate scientific data.

The success of any of these recommendations individually will be limited. What is needed is the adoption of an integrated national strategy that combines preventive measures (education, awareness-raising, economic opportunities) with remedial measures (legislation, security). Only through a comprehensive approach that recognises the social nature of cybercrime can Algeria move from a reactive policy to building lasting societal immunity against this ongoing threat.

9- Conclusion:

Cybercrime in Algeria is, in essence, a mirror reflecting the crises of contemporary Algerian society: the crisis of youth integration, the crisis of values under the weight of globalisation, and the crisis of socialisation institutions in the age of digitalisation. Therefore, any effective policy to curb this phenomenon must be comprehensive and integrated. Building ‘societal immunity’ against cybercrime necessarily involves rehabilitating the relationship between the individual and society, and between the citizen and the state, in both the real and virtual worlds.

10- Bibliography List:

- Agnew, R. (1992). Foundation for a General Strain Theory of Crime and Delinquency. *Criminology*, 30(1).
- Al-‘Ifa, A. (2021). Digital Identity and Hate Speech in Algerian Cyberspace: A Socio-Linguistic Approach. *University of El-Oued Journal of Social Sciences*, 5(2).
- Aubert, N. (2010). *The Hypermodern Individual*. Érès.
- Belaroussi, F. (2022). The Role of Peer Groups in Juvenile Delinquency in Urban Areas: A Field Study in Oran. *Journal of Social Sciences, University of Oran*, 10(1).
- Ben Omar, S. (2021). Consumer Culture and Algerian Youth Values in the Era of Globalization: A Sociological Field Study. *Journal of KasdiMerbah University – Ouargla*, 15(1).
- Benhamouda, M. (2020). Combating Cybercrime in Algeria: Assessment and Perspectives of the Legal Framework. *Algerian Journal of Law of Information and Communication Technologies*, 7(2).
- Benabdallah, K. (2021). Challenges of International Cooperation in Combating Cybercrime: The Case of Algeria. *International Conference on Digital Security, University of Oran*.

- Bouakkaz, S. (2023). Hate Speech in Algerian Cyberspace: From Political Conflict to Symbolic Violence. *Journal of Studies in Human and Social Sciences*, 9(1).
- Bouznina, S. (2021). Digital Transformation in Algeria: Issues and Opportunities. *Algerian Journal of Social Sciences*, 15(2).
- Bourdieu, P. (1986). The Forms of Capital. In J. Richardson (Ed.), *Handbook of Theory and Research for the Sociology of Education*. Greenwood.
- Boukhalfa, S. (2021). Social Networks and Identity Construction among Algerian Youth. *Insaniyat*, 85-86.
- Breton, P. (2000). The Cult of the Internet: A Threat to Social Bonds? *La Découverte*.
- Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, 44(4).
- Douidi, N. (2022). The Digital Divide in Algeria: Social Issues and Security Challenges. *Journal of Social and Human Sciences*, 28(1).
- Dubet, F. (2010). *Sociétés and School*. Seuil.
- ENISA (European Union Agency for Cybersecurity). (2022). *Cybersecurity Culture Guidelines: Behavioral Aspects of Cybersecurity*.
- Executive Decree No. 11-09 of January 3, 2011, Defining the Missions, Organization, and Operation of the National Office for Combating Cybercrime. *Official Gazette*, No. 2.
- Furnell, S. (2002). *Cybercrime: Vandalizing the Information Society*. Addison-Wesley.
- Hachani, A. (2020). Value Transformations in Algerian Society under the Influence of Globalization: A Sociological Study. *Journal of Batna University of Social and Human Sciences*, 8(2).
- Jaishankar, K. (2011). *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior*. CRC Press.
- Lagrange, H. (2010). *The Denial of Cultures*. Seuil.
- Livingstone, S., & Haddon, L. (2009). *Kids Online: Opportunities and Risks for Children*. The Policy Press.
- Merton, R. K. (1938). Social Structure and Anomie. *American Sociological Review*, 3(5).
- Ministry of National Education. (2022). *Middle and Secondary Education Curricula*.
- National Office for Combating Cybercrime (ONLCC). (2022). *Annual Report on Cybercrime*.
- National Authority for the Regulation of Telecommunications (ARPT). (2023). *Annual Report of the Telecommunications Sector*.
- National Office of Statistics (ONS). (2022). *Demographic Data for the Year 2022*.
- National Office for Combating Cybercrime (ONLCC). (2022). *Annual Cybercrime Statistics*.
- National Office for Combating Cybercrime (ONLCC). (2023). *Activity Report for 2022*.
- National Office of Statistics (ONS). (2023). *Labor Market Situation Report for 2022*. Statistical Bulletin 01/2023.
- Official Gazette of the Algerian Republic. (2009). Law No. 09-04 of August 5, 2009, on the Suppression of Crimes Related to Data Processing Systems, No:44.
- Sutherland, E. H. (1947). *Principles of Criminology*. J. B. Lippincott.
- Suler, J. (2004). The Online Disinhibition Effect. *Cyber Psychology & Behavior*, 7(3).
- Van Dijk, J. A. G. M. (2020). *The Digital Divide*. Polity Press. p. 3.
- Walklate, S. (2007). *Handbook of Victims and Victimology*. Willan Publishing.
- Yar, M. (2006). *Cybercrime and Society*. SAGE Publications. p. 4.