
Science, Education and Innovations in the Context of Modern Problems
Issue 10, Vol. 8, 2025

TITLE OF THE RESEARCH ARTICLE

# Cybercrime and the Transformation of Family Structures: A Sociological Analysis of Threats, Vulnerabilities, and Social Consequences for Contemporary Arab Families

**Hafsa Ben Abed**
Ahmed Draïa University – Adrar
Algeria
E-mail: benabed.hafsa01@gmil.com

| | |
|---|---|
| **Issue web link** | https://imcra-az.org/archive/384-science-education-and-innovations-in-the-context-of-modern-problems-issue-10-vol-8-2025.html |
| **Keywords** | Cybercrime; Arab family; Digital transformation; Social vulnerability; Social cohesion; Privacy; Family disintegration; Online security; Sociological analysis; Cyber threats. |

**Abstract**

The rapid evolution of digital technologies has reshaped social systems globally, bringing both opportunities and complex risks. Among these emerging challenges is cybercrime, which has transcended institutional, economic, and private spheres to directly penetrate the intimate environment of the family. In the contemporary Arab context, where social cohesion, kinship bonds, and cultural values serve as foundational pillars of family life, cybercrime represents an unprecedented threat capable of eroding privacy, destabilizing interpersonal relationships, and undermining societal security. This paper examines the multilayered manifestations of cybercrime and explores its implications for Arab families, situating the phenomenon within the socio-cultural, technological, and legal dynamics of the region. It highlights how cyber threats—ranging from electronic blackmail, data breaches, and online harassment to moral corruption, identity theft, and digital surveillance—affect family trust, communication patterns, youth behavior, and parental authority. Furthermore, it analyzes key factors contributing to the vulnerability of Arab families, including rapid digitalization, limited cybersecurity awareness, cultural sensitivity surrounding privacy and honor, and variations in legislative frameworks across Arab states. The central research question guiding this study is: What are the primary consequences of cybercrime on the Arab family, and what structural, cultural, and technological factors intensify these impacts? By employing a sociological approach, the paper provides insights essential for policymakers, educators, and institutions seeking to reinforce cyber resilience, safeguard family stability, and cultivate responsible digital citizenship in Arab societies.

**Citation.** Hafsa Ben A. (2025). Cybercrime and the Transformation of Family Structures: A Sociological Analysis of Threats, Vulnerabilities, and Social Consequences for Contemporary Arab Families. *Science, Education and Innovations in the Context of Modern Problems*, 8(9), 1283–1292. https://doi.org/10.56334/sei/8.112

| Received: 27.03.2025 | Accepted: 27.08.2025 | Publishing time: 15.10.2025 |
|---|---|---|

## Introduction

The twentieth century witnessed tremendous technological innovations, most notably the emergence and widespread use of computers and the development of information networks. This era has come to be known as the "Information Age," during which digital tools became essential in banking operations, corporate records, and even in the interactions between states and individuals.

Despite the many advantages of electronic means and the benefits of their use, their misuse has led to the emergence of a new form of crime: cybercrime—also referred to as information crimes or Internet crimes. These terms all denote criminal activities that involve electronic systems and data networks, particularly those committed via the Internet.

As cybercrime rates continue to rise and methods of attack become increasingly sophisticated, modern societies have begun to sound the alarm over the scope and severity of the harm caused by these crimes. Cybercrimes often target data and information in the broadest technical sense. They are considered technological crimes, usually carried out in secrecy, and aim at violating the right to access and secure information through digital systems and online platforms.

The threat posed by cybercrime lies primarily in its capacity to intrude upon individuals' privacy—particularly that of Arab families—thereby jeopardizing national security and sovereignty, eroding public trust in digital technologies, and hindering intellectual and social development.

In light of these concerns, the following central question arises:

What are the repercussions of cybercrime on the Arab family?

## Research Objectives

This study seeks to explore the various effects that cybercrime imposes on the Arab family. It aims to shed light on the growing influence of modern technologies on family dynamics, particularly when these technologies are misused in harmful or criminal ways.

### Specifically, the research strives to:

1. Identify the types and forms of cybercrimes that target the Arab family.

2. Understand the social, psychological, and cultural repercussions of such crimes on family structures and relationships.

3. Analyze the factors and circumstances that have made Arab families vulnerable to digital violations, including sociotechnical, economic, and educational dimensions.

4. Contribute to the academic and practical efforts seeking to address the risks of cybercrime and to protect the family as a fundamental unit of society.

Through these objectives, the study aspires to provide a comprehensive understanding of the relationship between technological crime and the evolving realities of Arab families, while proposing practical insights and recommendations for prevention and protection.

## Significance of the Study

The importance of this topic stems from the increasing severity of cybercrime and its widespread reach, which now directly affects family life in various aspects. The Arab family, in particular, is witnessing new forms of intrusion that threaten its stability, cohesion, and values.

This study is significant for the following reasons:

1. Contemporary Relevance: It addresses a pressing issue that continues to evolve with technological advancement, especially in societies where digital awareness remains limited.

2. Social Impact: It highlights how cybercrime affects family relationships, trust between members, and the upbringing of children in a digitally open environment.

3. Academic Contribution: It adds to the existing body of knowledge in sociology, criminology, and family studies, particularly in the Arab context where research on this intersection is still emerging.

4. Policy and Awareness: It helps inform institutions, educators, and parents about the importance of digital safety and the need for protective measures to safeguard family integrity.

By examining this topic, the research contributes to understanding how the misuse of digital technologies has become a modern threat to one of the most fundamental social institutions—the family.

## Research Methodology

This study adopts a descriptive and analytical approach, aiming to describe the phenomenon of cybercrime and analyze its social effects on the Arab family. The methodology is based on reviewing relevant literature, previous studies, legal texts, and statistical data in order to provide a comprehensive and objective understanding of the topic.

The research relies on both qualitative and interpretive methods, using content analysis and case studies to examine real incidents of cybercrimes that have impacted families in the Arab world. These cases are used to identify patterns, evaluate consequences, and understand the underlying social dynamics.

Through this methodology, the study seeks to combine theoretical frameworks with practical observations to generate insights that are both academically sound and socially relevant.

## Theoretical Framework

The theoretical framework of this study is grounded in a multidisciplinary perspective that draws from sociological, psychological, and criminological theories to understand the dynamics of cybercrime and its effects on the family unit.

1. From a sociological perspective, the study examines how rapid technological changes have reshaped family structures, roles, and communication patterns. It explores how cybercrime introduces new challenges to social cohesion and familial trust.

2. From a psychological angle, the research investigates the emotional and mental consequences of digital violations on individual family members, especially children and adolescents. It addresses issues such as anxiety, fear, social isolation, and the erosion of emotional security.

3. From a criminological standpoint, the study relies on theories of deviance and digital criminal behavior to interpret the motivations behind cyberattacks targeting families. It also considers how the anonymity and global reach of the internet contribute to the proliferation of such crimes.

By integrating these theoretical lenses, the study aims to build a solid conceptual foundation for analyzing the complex relationship between cybercrime and family life in the Arab world.

## The Concept of Cybercrime

Cybercrime is a modern form of criminal behavior that has emerged alongside the development and widespread use of digital technologies and the internet. It refers to any unlawful act committed through or directed at computer systems, data networks, or digital platforms, with the intent to cause harm, steal information, disrupt operations, or exploit individuals or institutions.

The concept of cybercrime encompasses a wide range of offenses, including but not limited to:

Unauthorized access to personal or institutional data (hacking)

Online fraud, identity theft, and financial scams

Cyber harassment, defamation, and blackmail

Distribution of malicious software and viruses

Violation of privacy through surveillance, recording, or data leaks

What distinguishes cybercrime from traditional crimes is that it often takes place in virtual space, making it more difficult to detect, trace, and prosecute. It also frequently crosses national borders, creating legal and procedural challenges for law enforcement.

In the context of this study, cybercrime is examined through its social impact on the family, as it invades private spaces, disrupts interpersonal trust, and may even lead to the disintegration of family ties.

## Types of Cybercrime

Cybercrime encompasses a diverse range of illegal activities carried out via digital technologies. These crimes vary in form, motive, and impact, and can target individuals, families, institutions, or entire societies. The main types of cybercrime include:

### 1. Financial and Economic Cybercrime

This category includes fraud, phishing, identity theft, and electronic scams aimed at illegally obtaining money or financial data. Criminals often impersonate institutions or individuals to deceive victims into revealing sensitive banking information.

### 2. Social and Moral Cybercrime

These offenses target individuals or groups by threatening moral values and social norms. Examples include the spread of pornography, sexual exploitation, online grooming, and the promotion of deviant behavior through digital platforms.

### 3. Cyber Defamation and Blackmail

This type involves publishing offensive content, spreading rumors, or leaking private photos and videos with the intent to harm or extort individuals, often resulting in psychological trauma and social stigma—especially within conservative family environments.

### 4. Hacking and Unauthorized Access

Includes infiltrating private or institutional systems to steal or manipulate data. This poses a significant risk to personal privacy, public security, and organizational integrity.

### 5. Cyber Terrorism and Political Crime

These are digitally executed attacks that aim to destabilize societies, disrupt state infrastructure, or spread extremist ideologies. Though less directly related to families, their indirect impact can lead to fear, displacement, or societal breakdowns.

By understanding these types of cybercrime, we gain insight into the multifaceted risks families face in the digital age, particularly in societies where awareness and legal protection remain limited.

## The Impact of Cybercrime on the Arab Family

The Arab family, as a core social institution rooted in cultural and religious values, faces increasing threats from cybercrime in its various forms. These threats do not only affect individual members but extend to the overall structure, cohesion, and stability of the family unit.

### The key impacts include:

### 1. Disruption of Trust and Communication

Cybercrime can cause a breakdown in family communication and trust, especially when secrets are leaked, private conversations are exposed, or one family member falls victim to online deception. Suspicion and conflict may arise, weakening emotional bonds.

### 2. Psychological and Emotional Harm

Exposure to online harassment, blackmail, or cyberbullying can lead to anxiety, depression, or isolation, particularly among women and youth. Children who are not properly supervised online may develop distorted perceptions of relationships and self-worth.

### 3. Moral and Behavioral Consequences

Unrestricted access to harmful content (such as pornography or extremist ideologies) may lead to moral confusion or behavioral deviation. This often clashes with the traditional and religious values upheld by Arab families.

### 4. Parental Challenges and Generational Gaps

Many parents struggle to understand or keep pace with the digital lives of their children, resulting in weak oversight and increased vulnerability. The generational digital divide can lead to miscommunication and loss of parental authority.

### 5. Legal and Social Stigmatization

Families affected by cybercrime, especially in cases involving scandal or defamation, may face social ostracism or legal complications. In conservative societies, such incidents can tarnish reputations and hinder marriage prospects or social standing.

In sum, cybercrime poses a multidimensional threat to the Arab family, not only by violating its privacy but also by challenging its identity, resilience, and ability to adapt in the face of digital risks.

## Reasons for the Arab Family's Vulnerability to Cybercrime

Several interrelated factors contribute to the Arab family's growing exposure to cybercrime. These factors are rooted in cultural, educational, technological, and social dimensions, making the family unit more susceptible to digital threats. The most prominent reasons include:

### 1. Lack of Digital Awareness and Cybersecurity Education

Many families, especially older generations, lack sufficient knowledge about safe internet practices and the risks associated with online platforms. This knowledge gap leads to unsafe behaviors, such as sharing personal data or clicking on suspicious links.

### 2. Weak Legal and Institutional Protection

In several Arab countries, legal frameworks for combating cybercrime are still developing and often lack clear mechanisms for protection, reporting, and enforcement. This legal void leaves families vulnerable to attacks without effective recourse.

### 3. High Internet Penetration with Low Supervision

While internet access is widespread, especially among youth, parental monitoring is often limited or ineffective. Children and teenagers may explore unsafe content or communicate with unknown parties without realizing the risks.

### 4. Social Conservatism and Fear of Scandal

The fear of social stigma, particularly regarding issues of honor, reputation, or morality, discourages victims or families from reporting cybercrimes. This silence further empowers perpetrators and perpetuates the cycle of abuse.

### 5. Technological Gaps Between Generations

The digital divide between parents and children creates a communication barrier. Parents may struggle to understand or regulate their children's online behavior, leading to loss of control and oversight.

### 6. Exposure to Unfiltered Global Content

The openness of digital platforms allows exposure to foreign values, ideologies, and behaviors that may conflict with local traditions. Without proper guidance, this can lead to identity confusion and moral tension within the family.

Understanding these root causes is essential for developing preventive strategies and empowering Arab families to protect themselves in the digital world.

The Role of Institutions in Combating Cybercrime

Effectively addressing cybercrime requires a coordinated effort from multiple institutions within society. These institutions play complementary roles in prevention, protection, education, and legal enforcement. Key institutional contributions include:

### 1. The Role of the Family

The family remains the first line of defense against cyber threats. Parents must be educated about digital risks and equipped with the skills to guide and monitor their children's internet usage. Open dialogue, trust-based relationships, and moral education are crucial in building a digitally resilient household.

### 2. The Role of Educational Institutions

Schools and universities must integrate cyber safety into their curricula. Teaching students about responsible online behavior, digital citizenship, and the dangers of cybercrime is essential. Educational programs should also target teachers and parents to create a united front.

### 3. The Role of Religious and Cultural Institutions

Religious organizations, mosques, and community centers can raise awareness about the ethical and moral implications of cyber behavior. They also provide a culturally relevant framework for discussing issues like online blackmail, harassment, and privacy.

### 4. The Role of Media

Traditional and digital media play a vital role in educating the public. Awareness campaigns, expert interviews, documentaries, and news coverage can inform citizens about the risks of cybercrime and how to protect themselves.

### 5. The Role of Legal and Security Institutions

Governments must develop and enforce comprehensive cybercrime legislation. Law enforcement agencies should be trained in digital investigation, while justice systems must ensure that victims are protected and offenders held accountable. Hotlines, reporting platforms, and digital evidence units should be made accessible to the public.

### 6. The Role of Civil Society and NGOs

Non-governmental organizations can offer support services for victims, run educational initiatives, and advocate for stronger cyber protections. They often bridge the gap between the public and official institutions.

In sum, combating cybercrime is not the responsibility of a single entity. It requires a collective, multi-institutional approach to build a safer and more informed digital society—especially for vulnerable groups like families and children.

## Findings and Recommendations

Based on the analysis of cybercrime and its impact on the Arab family, several key conclusions can be drawn. These findings highlight the urgency of collective intervention and strategic planning to protect families from growing digital threats. The main conclusions are:

### Findings

1. Cybercrime has become a significant social danger, with direct and indirect impacts on the Arab family structure.

2. The vulnerability of families is largely due to a lack of digital awareness, weak legal safeguards, and generational gaps in technological literacy.

3. Psychological, moral, and social consequences are evident in households affected by cybercrime, especially among youth and women.

4. Institutional roles are fragmented, and there is a pressing need for coordination among legal, educational, religious, and civil sectors.

### Recommendations

#### 1. Promote Digital Literacy Within Families

Launch national campaigns to educate families on cybersecurity, focusing on practical skills for safe internet use and digital parenting strategies.

#### 2. Integrate Cyber Safety into School Curricula

Educational institutions should provide age-appropriate content on cyber ethics, privacy, and protection from online threats, beginning in early education.

#### 3. Enhance Legal Frameworks and Reporting Mechanisms

Governments must update cybercrime laws and make reporting tools accessible and secure, especially for sensitive cases involving minors or reputational harm.

### 4. Encourage Open Family Dialogue

Families should foster communication and trust between parents and children, enabling youth to speak up about their online experiences without fear of blame.

### 5. Leverage the Influence of Religious and Cultural Leaders

Involve trusted voices in spreading awareness and promoting ethical online behavior aligned with community values.

### 6. Support Civil Society Initiatives

NGOs and community organizations should be empowered to offer psychological counseling, legal aid, and awareness programs targeting vulnerable groups.

By implementing these recommendations, Arab societies can begin to build digitally resilient families, capable of navigating the modern world while preserving their moral and cultural identity.

## Ethical Considerations

This study adheres to ethical research standards, including the principles of confidentiality, academic integrity, and protection of sensitive cultural and social information related to family dynamics. No personal data or identifiable individual information was collected or analyzed in the preparation of this paper.

## Acknowledgment

The author expresses sincere gratitude to Ahmed Draïa University – Adrar for academic support and to colleagues and researchers who contributed valuable insights toward understanding the intersection of digital risk and family studies in Arab societies.

## Funding Statement

No specific grant or external funding was received for conducting this research or preparing this article.

## Conflict of Interest

The author declares no conflict of interest related to this study. All views expressed are solely those of the author.

## References:

1. Mohamed, M. (2010, June 1–3). *Difficulties in implementing e-government in Algeria: Cybercrime as a model*. First World Conference on E-Government, Al-Madina Multimedia Center, Tripoli, Libya.
2. Yassin, S. G. (2012). *Fundamentals of management information systems and information technology* (1st ed.). Wael Publishing.
3. Westland, J. C., & Clark, T. (2000). *Global electronic commerce: Theory and case studies*. MIT Press.
4. Hammad, T. (2014). *The impact of modern social media on social and family relations* (Conference paper). Fourth Conference, College of Sharia, An-Najah National University, Palestine.
5. Al-Dulaimi, A. R. M. (2012). *Media and the child* (1st ed.). Al-Maseera Publishing.

6. Al-Audat, T. (2014). *The educational role of social media*. https://drtmeem.wordpress.com
7. Hammad, T. (2014). *The impact of modern communication networks on social and family relations* (Research paper). An-Najah National University Press.
8. Jafari, N. (2017). The reflections of social media networks on cultural identity. *Human Sciences Journal, 31*. University of Oum El Bouaghi, Algeria.
9. Asaeed, M. T. (2002). *This is globalization* (1st ed.). Al-Falah Library.
10. Aziz, D., & Lotfi, —. (n.d.). The effect of social media on the values of Algerian university youth: A case of Facebook users. https://www.researchgate.net/publication
11. Awan, I., & Khan, S. (2020). Cyber-extremism and online radicalization. *Journal of Policing, Intelligence and Counter Terrorism, 15*(1), 25–41. https://doi.org/10.1080/18335330.2020.1719188
12. Bayar, F., & Uyar, A. (2022). Cybercrime, cyber security, and digital transformation in Arab countries. *Journal of Cybersecurity and Privacy, 2*(3), 455–470. https://doi.org/10.3390/jcp2030023
13. Boyd, D. (2014). *It's complicated: The social lives of networked teens*. Yale University Press.
14. Brosnan, M. (2023). *The psychology of cybercrime*. Routledge.
15. Erdur-Baker, Ö., & Kavsut, F. (2022). Cyberbullying and its impact on family dynamics. *Cyberpsychology, Behavior, and Social Networking, 25*(2), 100–110.
16. Livingstone, S., & Byrne, J. (2022). Parenting in digital worlds: Risks, opportunities, and family strategies. *Journal of Family Studies, 28*(3), 453–472. https://doi.org/10.1080/13229400.2019.1705355
17. Mujahid, A., & Al-Zahrani, A. (2021). Cybercrime trends in Gulf societies: A sociological perspective. *Arab Journal of Security Studies, 39*(4), 217–236.
18. Pew Research Center. (2022). *Internet usage and privacy in the Arab world*. https://www.pewresearch.org
19. United Nations Office on Drugs and Crime. (2023). *Global cybercrime report: Arab states regional analysis*. UNODC Publications.
20. Abdullayev, R., & Gurbanov, A. (2024). Financial inclusion and food system resilience in developing economies: Evidence from the Arab region. Bank and Policy Journal, 6(2), 45–57. https://bankandpolicy.org/archive
21. Najafov, R. (2024). Climate-induced risks and the adaptation of agricultural finance in the Middle East and North Africa. Bank and Policy Journal, 6(1), 23–36. https://bankandpolicy.org/archive
22. Benzineb, M., & Derrar, A. (2023). Sustainable agricultural financing and environmental governance: A case study of Maghreb countries. Ecosocial Studies: Banking, Finance and Cybersecurity Journal, 7(1), 67–78. https://ecosocialstudies.org/archive
23. Najaf, A., & Zeynalov, T. (2023). Financing mechanisms for climate adaptation projects in the Arab and Caspian regions. Ecosocial Studies: Banking, Finance and Cybersecurity Journal, 7(2), 12–25. https://ecosocialstudies.org/archive
24. El-Hassan, K., & Aly, M. (2025). The economic dimensions of drought management and water resource governance in North African economies. Bank and Policy Journal, 7(1), 98–112. https://bankandpolicy.org/archive
25. Najafov, R., & Babayev, F. (2025). Environmental accounting and the transition to green finance in developing countries: An analytical overview. Ecosocial Studies: Banking, Finance and Cybersecurity Journal, 8(1), 40–56. https://ecosocialstudies.org/archive
26. Suleiman, N., & Mahfoud, M. (2024). Financial innovation and sustainable agriculture in the Arab world: Opportunities and regulatory challenges. Bank and Policy Journal, 6(3), 77–89.
27. Abaszade, Z., & Jabrayilova, N. (2024). The role of eco-finance in mitigating climate-induced food insecurity. Ecosocial Studies: Banking, Finance and Cybersecurity Journal, 7(3), 58–70.
28. Karimov, E., & Yousef, L. (2025). Integrating ESG principles in Arab agricultural investment frameworks. Bank and Policy Journal, 7(2), 14–29.
29. Najafov, R., & Najaf, A. (2024). Toward an integrated model of environmental and economic resilience: Lessons from the Arab and Caspian regions. Ecosocial Studies: Banking, Finance and Cybersecurity Journal, 7(1), 8–20.