LEX LOCALIS-JOURNAL OF LOCAL SELF-GOVERNMENT

ISSN: 1581-5374 E-ISSN: 1855-363X
VOL. 23 , NO. 10(2025)

Cybersecurity in the Digital Age: A Sociological Approach to Analysing Risks and Social Vulnerability

BOUZID Hacina
Baji Mokhtar Annaba, Algeria
Faculty of Humanities and Social Sciences
Department of Sociology
Email: bouzidhacina@yahoo.com
Received: 14/02/2025 *Accepted:10/07/2025* *Published: 02/10/2025*

Abstract

This study aims to analyse cybersecurity and digital vulnerability from a sociological perspective by examining the relationship between digital transformation and the social structures that shape cyberspace. The study begins with the premise that digital risks are not merely technical threats but also intertwined social phenomena arising from the interaction of digital awareness, behavioural patterns, and technological gaps within society. The significance of the research emerges in the context of the growing reliance on digital media, which has widened digital inequalities and led to the emergence of cyberthreats affecting individuals, institutions, and the state. The research draws on an analysis of previous studies addressing security awareness, digital identity, and cybersecurity governance, as well as on the use of three central theoretical approaches: Ulrich Beck's risk society approach, which interprets the production of digital risk in late modernity; Erving Goffman's symbolic interactionism, which helps explain the management of digital identity within the networked space; and Manuel Castells's network society approach, which highlights the role of digital networks in reshaping power and digital vulnerability. The findings indicate that digital vulnerability is shaped by several factors, most notably weak security awareness, the digital divide, limited digital literacy, and the absence of institutional cybersecurity governance. They also show that social institutions, particularly the family, education, and media, constitute a pivotal element in establishing sustainable digital protection and strengthening trust within the networked society. This study affirms that cybersecurity has become a fundamental pillar of social security and that understanding it from a sociological perspective is an essential entry point for managing digital risk and ensuring societal stability in an era of digital transformation.

Keywords: cybersecurity, digital age, social vulnerability, digital society, cyber risk

Introduction

The contemporary world is witnessing a profound transformation driven by the digital revolution, which has touched all areas of life, from the economy and politics to education and social communication. This transformation has led to the emergence of cyberspace as the new infrastructure of society, where human interactions and everyday practices are conducted through technological platforms that regulate our relationships with the world around us. In this context, cybersecurity has emerged as a central issue that cannot be overlooked, given its direct connection to the protection of information, data, and the digital identities of individuals and institutions. Notably, cybersecurity is, at its core, a fundamentally social issue that intersects with individuals' practices, perceptions, digital behaviour, and collective awareness of a new environment of risk. Herein lies the importance of approaching the subject from a sociological perspective, as it enables an understanding of the social structures that generate digital risk and the mechanisms through which vulnerability is reproduced within societies.

Cyberspace has become an open domain in which the real and the virtual intermingle, reshaping social relationships in profound ways. With this openness, a new type of threat that is not limited to malware or hacking but extends to multiple forms of digital violence, electronic extortion, information manipulation, and violations of privacy has emerged. Because these threats are not distributed equally among all users, it has become evident that some social groups are more exposed to risks than others are due to social, cultural, and cognitive disparities. Social vulnerability thus becomes a central concept for understanding how digital risk takes shape and how factors such as age, gender, level of education, and economic status influence individuals' ability to protect themselves within this complex digital environment.

Addressing cybersecurity in the digital age from a sociological perspective does not arise arbitrarily; somewhat, it is shaped by current challenges. On the one hand, technology has evolved rapidly, leaving individuals insufficient time to learn to use digital protection tools. On the other hand, societies are increasingly dependent on technological media in their various activities, making any security weakness a potential threat to individual and social safety. Moreover, the rise of socially driven cyberattacks such as social engineering, phishing, and violence directed against women and children reveals that digital risks are not merely technical but also bear precise social and cultural dimensions.

In addition, the importance of the sociological approach becomes evident, as cybersecurity cannot be ensured solely through technical tools but also through the cultivation of social awareness and responsible digital culture. The digital divide, for example, concerns not only the lack of access to technology but also the lack of knowledge and the ability to use it safely. This calls for a reconsideration of the role of social institutions in shaping individuals' digital behaviour and in strengthening or weakening their capacity to confront cyberthreats. Here lies the significance of a sociological reading: cybersecurity is the product of the interaction between technology and society, not merely a matter of technical tools and protection standards.

On the other hand, this subject is vital in light of the rapid transformations across the Arab world, where digital use has become an integral part of daily life but is often not

accompanied by sufficient security awareness or an adequate institutional framework to protect cyberspace. With the growing incidence of breaches, extortion, digital violence, and phishing, it has become essential to understand the social dimensions that render certain groups more vulnerable than others. Accordingly, approaching digital risk from a sociological perspective constitutes both a scientific necessity and a societal necessity, as it reveals the nature of the interaction between the individual and cyberspace and clarifies how risks emerge from within society itself.

Therefore, this article seeks to provide a comprehensive sociological reading of the concept of cybersecurity in the digital age by analysing emerging risks and interpreting the social vulnerabilities they create, with a focus on how social and cultural relations are reshaped within a transforming digital environment. The importance of this endeavour stems from the need to move beyond purely technical approaches and adopt a broader sociological perspective that considers cybersecurity as a structural issue shaped by societal culture, awareness, and patterns of interaction. Through this analysis, the article aims to contribute to the construction of a knowledge framework to understand the nature of the digital society and to propose new ways to enhance cybersecurity through a holistic social approach that transcends traditional technical solutions.

1. Problem Statement

The contemporary world is experiencing a profound transformation driven by the digital revolution and the widespread use of technology across daily life. Cyberspace is no longer merely a technical domain or a virtual communication arena; it has become a structural component of social life, shaping modes of interaction, the construction of relationships, and the production of symbols and cultures. Through this approach, individuals' behaviour is reshaped, new representations of identity are formed, and transboundary social networks are established. Within this increasing intertwinement between the social and the digital, the need has emerged to understand cybersecurity not only as a technical system that protects data and infrastructures but also as a social issue closely linked to cultural structures, collective values, and societal awareness.

The rapid development of technology has given rise to new forms of digital risk that extend beyond technical attacks to include social manipulation, social engineering-based methods, digital violence, privacy violations, and the exploitation of vulnerable groups through networks. This has made cybersecurity a fundamentally sociological issue, as these risks are not evenly distributed among users but are instead associated with levels of knowledge possession, digital competence, mental preparedness, and collective awareness. In this context, Ulrich Beck (1992), in his theory of *risk society*, affirms that technological progress itself produces new forms of risk that, over time, become part of social reality and cannot be separated from daily life. This corresponds to the condition of cybersecurity, which is not merely the product of technological systems but also a product of the structure and culture of society.

With the intensification of digital interaction, cyber vulnerability has emerged as an extension of traditional social vulnerability, as the degree of exposure to digital risk is

influenced by factors such as educational level, economic status, gender, generational differences, and available cognitive resources. The Arab researcher Nabil Ali (2003) noted that the digital transformation in Arab societies has not been sufficiently accompanied by the development of a robust digital culture, hindering individuals' ability to engage consciously with cyber risks. This confirms that digital threats are not merely technical but also primarily social in nature, extending beyond the boundaries of machines to connect with users' ways of thinking, perceptions, and cognitive preparedness.

The reasons for choosing this topic are not limited to the spread of new digital phenomena; they also include the fact that cybersecurity has become a component of societal security. Trust, which constitutes the core of social relations, has been threatened in cyberspace by the rise of digital deception, identity impersonation, the dissemination of misleading information, and the transformation of digital platforms into arenas for reproducing social inequalities. In addition, socially vulnerable groups (such as women, children, and the elderly) experience heightened vulnerability in the digital sphere due to limited technical knowledge and disparities in self-protection capabilities. Accordingly, we formulate the study problem through the following question:

How do social structures and digital culture contribute to the production of cyber vulnerability within the contemporary digital society?

This formulation enables reconsideration of the role of social institutions (the family, the school, and the media) as crucial actors in shaping digital awareness and building a societal culture capable of confronting the new threats posed by the digital age. On this basis, the following hypotheses were constructed:

1. Hypothesis One (H1): The digital divide increases individuals' exposure to cyber vulnerability within the digital society, as limited access to technology and digital skills renders certain groups more susceptible to digital exploitation.

2. Hypothesis Two (H2): The absence of security awareness as a social factor heightens individuals' vulnerability in the digital sphere, as unconscious behaviours such as sharing passwords or interacting with suspicious links intensify risks for vulnerable groups.

3. Hypothesis Three (H3): Social institutions (the family, the school, and the media) play a decisive role in reducing digital vulnerability, as coordination among them contributes to disseminating digital awareness and building collective resilience against cyberthreats.

Accordingly, addressing cybersecurity from a sociological perspective constitutes a scientific necessity for understanding the mechanisms through which risks are produced and confronted, as well as for identifying the role of culture and collective awareness in either strengthening or weakening digital protection. The importance of this perspective is heightened in Arab societies, where the digital and cognitive divide is continually

widening, rendering individuals more exposed to cyberattacks and manifestations of digital vulnerability.

2. Significance of the Study

- It reveals the sociological dimension of cybersecurity by analysing the relationship between technology and social structure and clarifying how technical risks have transformed into social risks that affect the stability of individuals and society.
- It highlights the role of social factors (such as age, education, and social status) in shaping levels of awareness of digital risk, thereby helping explain the varying capacities to protect digital identity across different social groups.
- It demonstrates the interconnectedness between cybersecurity and social security by showing how digital threats may evolve into broader societal threats.
- It deepens the understanding of digital vulnerability as a new form of social risk that requires multidimensional intervention.

3. Objectives of the Study

- To analyse the cyber phenomenon from a sociological perspective to understand how cybersecurity is linked to social structures and digital transformations in contemporary society.
- To identify the types of cyberthreats that exert the most significant impact on individuals and to determine how these threats are reflected in social relations and interactions within the digital space.
- To examine the role of social variables (age, educational level, and social status) in shaping levels of cybersecurity awareness and disparities among social groups.
- To assess individuals' levels of security awareness and their ability to protect their data and digital identities amid the widespread expansion of networked services.

4. Previous studies

4.1. Cybersecurity and Social Transformations in the Networked Society

Rainie, L., & Anderson, J. (2017). *The Future of Cybersecurity in the Networked Society*. Pew Research Centre.

This study examined the future of cybersecurity in networked societies, employing a descriptive analytical method based on a large-scale survey of experts in information security and digital sociology. The study revealed that cybersecurity threats have become embedded within the social structure itself, as they are not only related to technical attacks but also intersect with social trust, the management of digital identity, the spread of disinformation, and the widening gap in security awareness. The findings further indicated that individuals increasingly experience a state of "persistent uncertainty" regarding their data and their presence in digital space.

This study supports the article's sociological framework by demonstrating how cyberthreats have become an element reshaping social relations. It also exemplifies how cybersecurity can be understood as a social problem rather than merely a technical one.

2.4. Cybersecurity Awareness and Individuals' Digital Behaviour

Al-Hammadi, K. (2020). *Cybersecurity Awareness and Its Relationship to Social Behaviour on Social Media Platforms*. Contemporary Social Studies Journal, 12(3), 77–101.

This study aimed to measure the level of cybersecurity awareness among users of social media platforms and analyse its impact on patterns of digital behaviour. It employs a survey method in which a questionnaire is administered to a sample of university youth. The findings indicated that limited knowledge of digital risk is associated with increased risky behaviours, such as sharing personal data, accepting random friend requests, using weak passwords, and engaging with unknown links. The study also revealed that cybersecurity is linked to social behaviours such as trust, interaction, and engagement in digital life.

This study highlights the social dimension of cybersecurity and affirms the concepts of digital vulnerability and security awareness that I seek to analyse in my article. This finding demonstrates that social behaviour is inseparable from digital protection and that cybersecurity directly affects social relationships.

3.4. Digital Identity and Cyber Risks

Marwick, A., & Boyd, D. (2014). *Networked Privacy: How Youth Navigate Online Risks*. New Media & Society, 16(7), 1051–1067.

This study analysed how young people manage their digital privacy within networked environments through in-depth interviews employing a qualitative methodology. The authors found that the concept of privacy no longer means "concealing information" but has come to be linked to audience management, selecting what is displayed and what is hidden, and assessing the digital risks associated with identity. The study also highlighted that cyber risks are not merely technical but also involve social stigmatisation, the exploitation of images, electronic extortion, and peer surveillance.

This study is significant because it connects digital identity, a central theme in the theoretical framework, to the social cyber risks that threaten individuals. It provides academic legitimacy for analysing the relationship between cybersecurity and digital social identity.

4.4. The Importance of Cybersecurity Governance for Ensuring a Secure Digital Transformation of Public Services in Algeria

Zamoura, J., & Ben Aissa, Leila. (2022). *Importance of Cybersecurity Governance for Ensuring a Secure Digital Transformation of Public Services in Algeria*. Journal of Advanced Economic Research, 7(2), 414–429.

The study examines the trajectory of digital transformation in Algeria's public sector and demonstrates that the digitisation of public services (digital government services) exposes the sector to cyber threats. Moreover, the absence of strong cybersecurity governance is a significant weakness, as state digital institutions may be vulnerable to breaches without a clear strategic framework. The study further indicates that Algeria requires a coherent regulatory framework, along with technical and human mechanisms, to strengthen cybersecurity in public digital services and protect citizens' data and official information.

The study proposes adopting “practical models and frameworks” for cybersecurity governance, including training qualified personnel, applying international security standards, and establishing institutional policies to protect critical infrastructures.

This study is directly related to the concept of digital vulnerability from an institutional perspective, as it shows how governmental infrastructures can be “cyber vulnerable” if security is not properly governed. It also demonstrates that digital transformation is not merely an economic or administrative objective but becomes a societal risk if it is not accompanied by strong security governance. This finding reinforces the idea that cybersecurity is an integral component of social stability.

5. The Theoretical Approach

This research draws upon a set of theoretical approaches that enable the understanding of cybersecurity as a complex social phenomenon that transcends its technical dimension and extends into the symbolic and organisational structures of the digital society. Accordingly, understanding security transformations in the digital world requires multiple sociological perspectives that reveal how cyberspace reshapes identity and social relations, drawing on central approaches to construct an integrated interpretive framework of the phenomenon.

5.1. The Sociological Approach to Risk (Ulrich Beck – Risk Society)

This approach is based on analysing the nature of modern risks, particularly those that are “socially produced” and characterised by immateriality, global reach, and unpredictability. In risk society, Ulrich Beck notes that risks in late modernity include informational threats that escape traditional forms of protection, creating a continuous state of "digital uncertainty" (Beck, 1992, p. 37).

This perspective helps explain how cyberattacks and data leaks have become sources of collective fear and how societies have become more preoccupied with managing digital risk than with addressing traditional social conflicts.

5.2. Symbolic interactionism and digital identity (Goffman–Symbolic interactionism)

This theory provides an important framework for understanding how individuals construct their digital identities. According to Erving Goffman, individuals manage their "social front" in everyday life through what he terms the "presentation of self" (Goffman, 1959, p. 22). In the digital environment, this front becomes more fragile because the individual's identity is transformed into data, images, and interactions that can be easily manipulated or compromised.

This perspective helps explain how cybersecurity becomes essential to protecting identity and how weak digital protection leads to the erosion of trust, heightened feelings of surveillance, and changes in social interaction patterns.

5.3. Network Society Theory (Manuel Castells – Network Society)

Castells provides a comprehensive vision of the digital age as an age of networks in which social, economic, and political structures are governed through transboundary information systems. Castells noted that "networks are the fundamental structure of the new society" (Castells, 2010, p. 21), which makes cybersecurity a prerequisite for the stability of social relations.

This perspective helps in understanding how the complexity of digital networks expands the surface of cyber vulnerability and gives rise to new actors (hackers, organised groups, technology companies, algorithms) who reshape the concept of power.

The Conceptual and Theoretical Framework

First: Defining the Concepts

1. The Concept of Cybersecurity

Cybersecurity is one of the central concepts shaping the structure of modern digital life. It refers to the set of methods, tools, and procedures designed to protect information, data, networks, and electronic systems from attacks and breaches. However, the sociological approach views this concept within a broader context than the technical frame does, considering it a fundamental element of societal stability and of society's ability to adapt to the digital environment. According to Whitman and Mattord (2022, p. 17), cybersecurity is defined as "a collection of policies and technical and organisational means aimed at protecting informational assets from internal and external threats." Singer and Friedman (2014, p. 51) also emphasise that cybersecurity "is no longer merely a technical field but has become an arena related to national security and social behaviour within networks."

From the perspective of digital sociology, cybersecurity transcends its protective dimension to include the influence of technology on social trust, identity, and power.

Castells (2010, p. 221) noted that controlling information within a networked space constitutes a form of power in digital society. Thus, cybersecurity becomes a tool for regulating this space and ensuring its stability. In the same context, Kello (2017, p. 74) explains that cyber attacks “directly affect social and political relations,” highlighting the importance of understanding the nature of these threats and their long-term implications.

Bayuk (2011, p. 33) further stresses that cybersecurity requires a social understanding of digital behaviour, not merely technical knowledge of network infrastructures. The human factor is the central vulnerability in the security system, as users' daily decisions determine the level of risk. Therefore, societal security in the digital age is directly linked to cybersecurity, an interwoven sociotechnical system shaped by the interaction between humans and technology, rather than a set of rigid protective tools.

2. The Concept of the Digital Society

The digital society represents a new stage of social development in which technology intersects with all aspects of daily life, from education and work to communication and entertainment and from the economy to politics. Debray (2017, p. 15) noted that digital society is "a society in which digital technologies shape the structure of social relations and in which electronic media reshape patterns of production and interaction." The distinctiveness of this society lies in its reliance on flows of information rather than traditional structures. This aligns with Castells's (2010, p. 145) description of the "network society," in which power is built upon communication capacities rather than material resources.

From a sociological perspective, the digital society does not merely entail the use of technology; it denotes a profound reorganisation of social relations in which new concepts emerge, such as digital identity, digital citizenship, synchronous interaction, and the immaterial economy. Lévy (1999, p. 63) argues that the digital society forms “a knowledge society” grounded in the production and circulation of information, creating new spaces for belonging and representation. This indicates that social life has moved beyond natural physical space into virtual domains that offer multiple possibilities for presence.

As Ritzer (2021, p. 112) discusses, the notion of "digitally empowered individuals" refers to users who produce content and interact within expansive networks, making the digital society a distinctly participatory one. However, Fuchs (2014, p. 98) noted that this society also encompasses new forms of control and surveillance, as digital platforms can shape behaviour and regulate the flow of data. This renders digital society not only a space of freedom but also a space of subtle domination.

Accordingly, digital society is a new social framework in which relations, power, and identities are reconfigured, and cybersecurity becomes an essential prerequisite for maintaining cohesion and stability.

3. Concept of Cyber Vulnerability

Cyber vulnerability refers to the susceptibility of individuals or institutions to digital breaches or electronic threats, driven by technical, social, or behavioural factors. Cavelty (2015, p. 112) defines cyber vulnerability as "a weakness in the information system or in the user's behaviour that permits a breach or potential harm." This vulnerability is not limited to technical systems but also extends to a lack of awareness, limited digital literacy, educational gaps, and everyday usage errors.

According to Clarke and Knake (2010, p. 71), cyber vulnerability is a direct consequence of increased dependence on technology without the development of appropriate protection capacities. They stress that "society's reliance on digital media is increasing far faster than its ability to protect itself." This makes social groups with lower levels of education and culture more vulnerable to cyber threats. Boyes (2019, p. 88) indicates that cyber vulnerability comprises three levels:

- **Technical vulnerability:** weaknesses in systems and devices.
- **Human vulnerability:** lack of awareness and susceptibility to fraud.
- **Institutional vulnerability:** insufficient policies and organisational structures.

Anderson (2020, p. 52) noted that "the human factor accounts for 70% of breaches," reflecting the central role of behaviour in shaping vulnerability. Lewis (2018, p. 132) further noted that cyber vulnerability is exacerbated by the spread of rumours and electronic fraud, particularly in societies with weak digital cultures, leading to a deterioration of trust in digital space and in social relations.

Accordingly, cyber vulnerability is a key element in understanding cybersecurity from a social perspective, as it explains why risk levels vary among individuals and how the digital divide is reproduced within society.

Second: Types of Digital Risks

Digital risks constitute one of the most prominent challenges arising from rapid technological transformations, as electronic environments have become spaces in which technical, behavioural, and organisational threats intersect. These risks can be classified by their nature, source, and impact on individuals, society, and institutions.

1. Technical Risks

Technical risks include cyberattacks, breaches, and software vulnerabilities that may result in data loss or service disruption. These risks include viruses, malware, distributed denial-of-service (DDoS) attacks, and the exploitation of security flaws, including zero-day vulnerabilities (Reddy & Ugander Reddy, 2014, p. 5). Their severity is particularly evident in institutions that rely on inadequately protected information systems, where any breach can disrupt services and directly affect society's digital security.

2. Behavioural Risks

These risks are linked to users' behaviour within the digital environment, such as sharing personal information, accepting unknown friend requests, or interacting with suspicious links. Studies have shown that low security awareness increases the likelihood of cyberattacks such as electronic extortion and cyberbullying (Evans, Maglaras, He, & Janicke, 2016, p. 12). This category of risk highlights individual vulnerability to digital threats and their effects on trust within digital spaces.

3. Organisational digital risks

Institutions experience specific organisational risks due to weak internal policies or the absence of clear cybersecurity strategies. These risks include poor management of employees' digital identities, lack of protection protocols, and inadequate emergency response plans (Mansouri, 2022, pp. 265–270). Such risks may lead to disruptions in public services or the loss of strategic data, placing society as a whole at risk of digital deterioration.

4. Sociodigital Risks

These risks concern the effects of digital environments on social relations, including the spread of rumours and fake news, social polarisation, and involvement in digital pressure groups. They focus on how the digital environment influences mental health and social trust (Bada & Nurse, 2019, p. 1055). These risks also affect the quality of public digital discourse and individuals' ability to interact freely and safely.

5. Economic Digital Risks

Economic digital risks include electronic fraud, theft of banking identity, ransomware attacks, and the disruption of commercial operations. Studies have shown that SMEs are more exposed to these risks because of their limited capacity to protect data (McKinsey & Company, 2024). These risks directly affect market stability and the financial security of the digital society.

6. Legal and privacy risks

These risks are related to noncompliance with laws governing personal data protection and intellectual property rights, as well as the exploitation of personal data for commercial purposes without consent. The absence of appropriate legislation in some countries contributes to increased cyber vulnerability and poses a direct threat to individual privacy and the stability of digital society (Mansouri, 2022, pp. 270–272).

7. Ethical Digital Risks

Ethical risks arise from the disconnect between traditional values and digital practices, such as the spread of unethical content, violence in online games, or the irresponsible use of artificial intelligence. These risks particularly affect vulnerable groups, including

children and adolescents, and contribute to the reinforcement of long-term digital vulnerability (Bada & Nurse, 2019, p. 1060).

Third: Social Factors Producing Digital Vulnerability

Digital vulnerability is a contemporary social phenomenon that emerges from the complex interactions between technology and society. Risks are not limited to technical dimensions; they are also influenced by social factors that determine individuals' and groups' ability to protect themselves against digital threats. These factors may be classified as follows:

1. Weak Digital Culture and Awareness

Weak digital awareness is one of the most significant social factors producing digital vulnerability. Many users lack sufficient knowledge regarding data protection methods, password management, and the identification of fraudulent links or malicious software. According to Al-Hammadi (2020), users' lack of awareness of digital risks leads to dangerous behaviours, such as careless sharing of personal information, increasing their susceptibility to cyberattacks and cyberbullying (Al-Hammadi, 2020, pp. 82–84). Digital awareness, therefore, emerges as a fundamental factor in reducing individual and collective vulnerability within the digital society.

2. Social and Economic Inequality

This form of inequality concerns the economic and educational capacity to access modern technology and use it safely. Individuals with low incomes or limited educational attainment often lack the tools and expertise to protect themselves, thereby increasing their exposure to risks. Mansouri's (2022) study shows that less-equipped institutions and individuals face greater threats due to weak digital governance and insufficient cybersecurity training (Mansouri, 2022, pp. 265–267).

This demonstrates that digital vulnerability is not merely a technical issue but is strongly connected to the social and economic structure.

3. Widespread Unaware Use of Social Media Platforms

Social media networks significantly contribute to the production of digital vulnerability, as excessive or unconscious use exposes users to risks related to privacy, misinformation, and engagement in harmful groups. Marwick and Boyd (2014) indicate that young people tend to share their personal lives openly, increasing their likelihood of exposure to extortion or digital impersonation (Marwick & Boyd, 2014, p. 1055). Thus, digital social interaction becomes a direct social factor in shaping vulnerability.

4. Weak Governance and Digital Socialisation

These factors are related to the absence of institutional or familial guidance in teaching individuals how to interact safely within digital environments. Families, schools, and institutions often lack awareness programmes and guidance on cybersecurity, leading individuals to develop unsafe internet habits. According to Bauman and Lyon (2013), contemporary digital society lives under continuous surveillance, and vulnerability often results from the absence of effective regulatory and educational frameworks to protect individuals (Bauman & Lyon, 2013, p. 45).

5. General Social and Cultural Factors

These factors include prevailing social values, patterns of collective interaction, and the general level of trust in technology and institutions. Societies with low levels of trust in digital institutions often struggle to enforce collective protection practices, which increases individuals' and groups' exposure to cyberattacks (Beck, 1992, pp. 39–41). Additionally, social values related to privacy and transparency influence the extent to which individuals comply with digital security procedures.

Accordingly, these factors demonstrate that digital vulnerability is not merely the result of technical flaws but also a social phenomenon rooted in culture, education, economic inequality, everyday digital practices, and weak governance. Understanding these social factors is essential for developing effective strategies to reduce digital risk and protect individuals and society.

Fourth: Groups Most Vulnerable to Digital Risks

Digital vulnerability varies among individuals and groups depending on age, educational level, technical experience, and socioeconomic disparities. Several groups stand out as being particularly targeted within the digital society, making them more exposed to digital risk.

1. Children and Adolescents

Children and adolescents are among the groups most vulnerable to digital risk because of their limited experience and understanding of electronic threats. They use the internet for social communication, online games, and interactive content without fully comprehending the risks of privacy breaches, extortion, or digital impersonation (Livingstone & Smith, 2014, pp. 7–9). Studies indicate that excessive exposure to digital platforms renders this group susceptible to electronic extortion, cyberbullying, and adverse effects on their psychological and social well-being.

2. Youth and University Students

University-aged youth engage heavily with digital media and rely heavily on smartphones and social media platforms for learning and social interaction. With this intensive use, the likelihood of exposure to digital extortion, identity theft, or the exploitation of personal data increases (Marwick & Boyd, 2014, p. 1055). Al-Hammadi's

(2020) study also showed that low security awareness among students increases risky behaviours such as sharing passwords or accepting suspicious friend requests, reflecting the vulnerability of this group to digital threats (Al-Hammadi, 2020, pp. 83–85).

3. Older Adults

Older adults face difficulty adapting to modern technology because of limited digital experience and a lack of knowledge about data protection methods. They commonly do not use protective tools such as antivirus software or regular security updates, making them susceptible to financial fraud, phishing messages, and digital manipulation (Charness & Boot, 2009, p. 120). Older adults are also economically targeted because of their low awareness of digital threats.

4. Groups Facing Economic and Educational Gaps

Individuals with limited income or lower educational levels often lack access to digital protection tools and solutions, such as secure networks, cloud computing, or digital training. Mansouri (2022) noted that these groups suffer from weak digital governance, making them more exposed to cyberattacks targeting personal and institutional data (Mansouri, 2022, pp. 265–268).

5. Workers in Sensitive Digital Institutions

Employees in banks, government institutions, and technology companies are particularly vulnerable to digital risk, as breaches of their systems can cause widespread harm. The human factor plays a significant role in digital vulnerability, particularly when cybersecurity training is insufficient or when information protection protocols are ignored (Evans, Maglaras, He, & Janicke, 2016, p. 12).

Accordingly, these groups illustrate that digital vulnerability is not uniform but is instead shaped by digital experience, age, educational level, and economic status. Identifying these targeted groups is essential for developing tailored awareness and protection strategies that reduce digital risk at both the individual and collective levels.

Fifth: Social Vulnerability in the Digital Age

1. Digital Inequality and Its Role in Producing Cyber Vulnerability

In the digital age, the digital divide is one of the most significant structural factors contributing to the development of cyber vulnerability. This divide is not limited to internet access; it also concerns the ability to understand and use technology and digital services effectively and safely. Unequal access among economically, geographically, or educationally disadvantaged groups creates a real gap in the possession of the "digital capital" necessary for self-protection in cyberspace. According to international researchers, digital divides reinforce traditional social inequalities within the digital sphere (Ragnedda & Muschert, 2013, p. 45). Individuals who lack digital training or

technical skills are more exposed to cyber risks because they lack the knowledge to address threats or implement effective protection strategies.

From a local perspective, in Algeria, studies indicate that digital transformation faces challenges related to unequal digital infrastructure between urban and rural areas, which increases certain groups' vulnerability to attacks or privacy violations (Ben Berghout, 2023, p. 446). The disparity in connection quality and speed and the lack of stable internet access in some regions make these spaces "fragile zones" that are more susceptible to breaches or digital exploitation.

Furthermore, research highlights that education plays a central role in bridging the gap between digital inequality and cyber vulnerability. Individuals with low digital skills tend to be passive consumers of digital services and are unable to understand potential risks or formulate personal security strategies (Lahiri, 2024, p. 10). This compels societies to invest in digital training to empower disadvantaged groups and reduce the digital vulnerability gap. Societies that overcome the digital divide are better equipped to build collective resilience against cyber threats.

2. Absence of Security Awareness as a Social Factor

One of the essential social factors contributing to individuals' vulnerability in the digital space is a lack of digital security awareness. This awareness goes beyond knowledge of a few technical rules; it encompasses a culture of interacting with technology safely, for example, using strong passwords, verifying links, avoiding phishing attempts, and regularly updating software.

From an international perspective, studies in digital sociology indicate that users who do not possess strong security awareness are more vulnerable to socially engineered attacks, such as social engineering and phishing, because they fail to recognise the risks associated with sharing their data or accepting unknown friend requests (Lahiri, 2024, p. 12). This lack of awareness becomes a form of cyber weakness, as it provides attackers with opportunities to exploit human behaviour, which is often the weakest link in the security chain.

At the Algerian level, research shows that many users lack sufficient knowledge of cybersecurity concepts, with some believing that simply using a password is enough to protect their accounts. In their study on cyberthreats in Algeria, Zawawi and Ramli (2023, p. 150) revealed that the absence of digital education reinforces poor security practices, such as using simple passwords, reusing the same password across multiple accounts, or sharing devices with others. This lack of digital security awareness stems not solely from limited technical knowledge but also from the absence of an established digital culture in many societies, making cyber vulnerability the result of a social and cultural structure rather than a purely technical shortcoming.

Moreover, the absence of security awareness affects not only individuals but also institutional efficiency. Many employees in public or private institutions lack adequate

training to address digital risk. This creates a significant point of weakness within institutions, one that attackers can exploit, placing institutional data at risk and weakening their capacity to respond effectively to cyberattacks.

3. The Role of Social Institutions in Strengthening Protection

Many social institutions, such as families, schools, and media, play crucial roles in developing "digital social immunity" against cyber vulnerability. Without the combined efforts of these institutions to cultivate a culture of digital security, individuals confront digital threats alone, increasing their exposure and risk.

First, the family:

The family is the primary environment for children and adolescents, and it is the setting in which digital safety values can be established from an early age. When families create an environment where digital risks are discussed and children are taught to behave safely in digital spaces, early awareness develops, helping to form sustainable protective practices. When families neglect this responsibility, children may grow up without sufficient understanding of the dangers of sharing information or interacting with strangers, making them vulnerable to attacks such as impersonation or extortion.

Second, the school:

As educational institutions, schools play a central role in building digital competencies and security knowledge. By integrating digital education into school curricula, schools can teach learners about cyber threats, data protection methods, and ethical digital behaviour. Foreign studies indicate that digital education is not limited to technical skills but includes forming an informed view of security and privacy (Ragnedda & Muschert, 2013, p. 120).

In the Algerian context, there are increasing calls for schools to strengthen students' security awareness, as the absence of such training creates fertile ground for digital vulnerabilities.

Third, the media:

Digital media institutions can serve as practical tools for raising security awareness. Through awareness campaigns, digital literacy programmes, and journalistic reports on cyber risk, the media can demonstrate social responsibility by guiding users towards safe practices. In Algeria, studies on cyberthreats confirm that digital media can contribute to building collective security awareness when its messaging is systematically employed (Zawawi & Ramli, 2023, p. 154).

Moreover, coordinating the efforts of these institutions, families, schools, and media is essential for achieving comprehensive and realistic protection. Each contributes to establishing a shared culture of digital security rather than isolated individual training.

Without this coordination, efforts remain fragmented and may fail to build strong digital immunity within society, thereby increasing long-term cyber vulnerability.

In conclusion, social vulnerability in the digital age arises from the interaction of several factors: inequality in access to technology, the absence of security awareness, and the weakened role of social and educational institutions. To build a safer digital society, technical measures alone are insufficient; instead, a comprehensive strategy that connects social, cultural, and organisational dimensions is needed. Digital transformation must be accompanied by security-oriented socialisation so that cybersecurity becomes part of the everyday life of every individual.

The Analytical and Sociological Dimension

1. Sociological Analysis Based on Previous Studies

1.1. Analysis of Rainie & Anderson (2017)

The study by Rainie and Anderson (2017) examines the future of cybersecurity in networked societies. This reveals that cyber risk is no longer confined to the technical dimension but has become an integral part of the social structure itself. The sociological analysis of this study shows that social trust, digital identity management, and the spread of disinformation all influence how individuals perceive digital risk. The state of "persistent uncertainty" experienced by users indicates a reshaping of social relations within the digital society, where social trust intersects with cyber risk.

From a sociological perspective, this means that digital vulnerability is not merely a technical weakness but also an interwoven social phenomenon emerging from individuals' everyday interactions with digital space, whether through data sharing or engagement with misleading content. The study also shows that cybersecurity has become a factor in social stability; the absence of protective frameworks weakens trust between individuals and institutions and increases the complexity of digital interactions.

1.2. Analysis of Al-Hammadi (2020)

Al-Hammadi's (2020) study focused on cybersecurity awareness and the digital behaviour of university youth. The sociological analysis shows that insufficient knowledge of digital risk leads to dangerous behaviours, such as sharing personal data or clicking on unknown links, thereby increasing an individual's digital vulnerability within the digital society.

From a social standpoint, digital behaviour is linked to concepts of trust, interaction, and engagement in digital life, which means that cybersecurity is not solely a technical matter but is tied to digital culture and social relations. A lack of security awareness leads to risk-prone behaviours, thereby amplifying digital vulnerability across society. The study also confirms that educating and raising individuals' awareness of digital risk is an

essential component of social and cyber protection strategies, as individual behaviour directly affects the overall level of collective security.

3. Analysis of Marwick & Boyd (2014)

The study by Marwick and Boyd (2014) examined how young people engage with digital identity and the risks associated with it. The sociological analysis indicates that digital privacy is no longer limited to concealing information; it has become part of managing one's social identity online. Young people choose what to reveal and what to conceal, navigating risks such as extortion, exploitation of images, and peer surveillance.

This highlights that digital vulnerability is intertwined with digital social identity and that seemingly simple actions in the digital space can lead to significant social and psychological harm. From a sociological perspective, this study shows that cybersecurity is linked to power relations and social stigmatisation within the digital society and that the conscious management of digital identity constitutes a renewed mechanism of social protection.

4. Analysis of Zamoura & Ben Aissa (2022)

Zamoura and Ben Aissa (2022) address the importance of cybersecurity governance in the digital transformation of public services in Algeria. The sociological analysis shows that the absence of strong governance renders governmental infrastructure cybervulnerable, thereby directly affecting society as a whole, as official data and digital services become susceptible to breaches.

From a social perspective, this reflects that digital transformation is not merely an economic or administrative objective but also a societal risk if not accompanied by a comprehensive security framework. Digital vulnerability within public institutions undermines citizens' trust in digital services, thereby reproducing weakened social trust. The study confirms that adopting practical governance models and frameworks, training qualified personnel, and regulating institutional security policies can transform threats into digital social protection, thereby enhancing the stability of the digital society as a whole.

2. Analysis according to the theoretical approaches

2.1. The Sociological Approach to Risk (Ulrich Beck – Risk Society)

Beck's approach emphasises that risks in modern societies are not random events but socially produced risks characterised by immateriality, unpredictability, and widespread societal impact (Beck, 1992, p. 37). In the digital age, such risks include cyberattacks, data leaks, and the proliferation of digital misinformation phenomena that cannot be controlled through traditional security measures.

The sociological analysis indicates that these risks create a state of "digital uncertainty" for individuals and shape societal trust in digital institutions and platforms, thereby reshaping the social structure itself. Digital vulnerability emerges from multilevel interactions: inequalities in access to technology, weak digital education, disparities in individuals' ability to protect personal data, and social behaviors that heighten risk exposure.

Smith and Duggan (2019) demonstrated that individuals who use the internet intensively without adequate digital awareness are more likely to experience breaches and digital extortion and that such experiences have lasting effects on their social relationships and their trust in digital platforms (Smith & Duggan, 2019, p. 45).

Continuation of the Analytical and Sociological Dimension

2.1. Completion of the Risk Society Approach (Ulrich Beck)

Accordingly, Beck’s framework provides a basis for understanding that cybersecurity is not merely a technical tool but also a component of managing modern social risk and that digital vulnerability reflects underlying social and cultural disparities. This perspective also clarifies that digital policies cannot be effective unless they address the broader social structure that produces vulnerability, including the family, the school, the media, and the digital inequalities between individuals.

2.2. Symbolic interactionism and digital identity (Goffman–Symbolic interactionism)

Goffman's theory emphasises that individuals manage their "social front" and perform a "presentation of self" within daily interactions, which is consistent with social expectations (Goffman, 1959, p. 22). In the digital environment, this social front becomes more fragile, as data, images, and interactions are transformed into content that can be easily manipulated or compromised. This makes cybersecurity an essential element in protecting both individual identity and social identity.

Thus, weak digital protection clearly leads to the erosion of trust among individuals, heightened feelings of surveillance and continuous social evaluation, and altered patterns of digital interaction. A study by Van Dijck and Poell (2015) confirmed that users continuously manage their digital identities, regulating what is displayed and what is concealed on the basis of potential risks and social relationships. This demonstrates that digital behaviour is directly linked to social awareness and digital security (Van Dijck & Poell, 2015, p. 78).

From this perspective, digital vulnerability emerges from the interaction between technical capacities and social behavior. A person may be exposed to risks not only due to weak technological safeguards but also to poor management of their digital identity in social interactions. This analysis highlights the importance of teaching individuals digital

self-regulation skills and strengthening a digital security culture, making cybersecurity an integral part of broader social protection strategies.

2.3. Network Society Theory (Manuel Castells – Network Society)

Castells argues that networks constitute the foundational structure of the digital society and that the informational paradigm has rendered digital security a prerequisite for the stability of social, economic, and political systems (Castells, 2010, p. 21). The sociological analysis shows that the complexity of digital networks expands the surface of cyber vulnerability, with new actors, such as hackers, organised groups, technology companies, and algorithms that govern information flows and reproduce power structures, emerging.

A study by Rainie and Wellman (2012) revealed that networked societies rely fundamentally on digital trust, and any cybersecurity breach erodes this trust, weakening social bonds within networks and increasing individuals' and institutions' vulnerability (Rainie & Wellman, 2012, p. 56).

Consequently, cybersecurity is not simply technical protection but rather a vital element for the stability of the entire network society, as it reflects the ability of individuals and institutions to safeguard their data and interact with confidence across networked environments.

From this perspective, the analysis indicates that digital vulnerability is not merely an individual issue but rather the outcome of a complex, interconnected social structure that includes digital education, community awareness, governance policies, and the participation of social institutions in building a culture of digital security. These elements collectively strengthen the stability of the digital society and reduce risks for individuals and the community as a whole.

3. Analysis According to the Central Question and Hypotheses

The articulation of the study's central problem demonstrates that cyber vulnerability is not the result of purely technical factors but rather a product of the interactive relationship between social structure and digital culture. Digital societies reflect individuals' everyday interactions, in which social values, cultural practices, and digital behavioural patterns shape the degree of exposure to risks. This includes the family's role in guiding digital use, the school's role in digital education, and the media's role in disseminating information and strengthening security awareness.

Thus, understanding digital vulnerability requires a sociological reading that links the individual, institutions, and broader digital society, not merely a technical analysis of attacks or malicious software.

3.1. Analysis of Hypothesis One (H1): Digital Inequality Increases Individuals' Exposure to Cyber Vulnerability

Hypothesis One posits that gaps in access to technology and digital skills increase the exposure of vulnerable groups to cyberthreats. The sociological analysis indicates that this divide is not simply a technical deficit but also reflects traditional social divisions such as education, income, and social status. Individuals who lack continuous access to digital technologies or who do not possess the ability to protect their data experience compounded vulnerability and become more prone to extortion, fraud, and privacy violations.

From this perspective, cybersecurity reflects a social challenge that links digital inequality to social stability and emphasises that digital policies must address inequality as part of broader social protection strategies.

3.2. Analysis of Hypothesis Two (H2): Absence of Security Awareness Increases Individual Vulnerability

This hypothesis posits that unconscious behaviours in digital spaces, such as sharing passwords or clicking on unknown links, increase individuals' exposure to cyber risks. The sociological analysis indicates that the absence of security awareness results from interactions among family-based digital education, school curricula, and broader socialisation processes. The weaker the degree of digital education is and the lower the emphasis on security awareness is, the greater the sense of vulnerability among users.

Therefore, cybersecurity is directly linked to social behaviour and digital culture. It influences individuals' level of trust, their ability to protect themselves, and the overall stability of the digital society.

3.3. Analysis of Hypothesis Three (H3): Social Institutions Play a Decisive Role in Reducing Digital Vulnerability

Hypothesis Three emphasises that the family, the school, and the media constitute key actors in building digital awareness and strengthening individuals' protection against cyber risk. The sociological analysis shows that cooperation among these institutions can significantly reduce individuals' exposure to vulnerability:

- The **family** provides guidance and emotional support,
- The **school** offers awareness programmes and digital literacy training, and
- The **media** disseminates accurate information that helps users avoid risks.

Thus, digital vulnerability is not an inevitable fate but rather the outcome of weak social and cultural coordination. Strengthening the role of social institutions is a vital strategy for transforming digital society into a safer environment, making cybersecurity an integral component of social structure rather than merely a technical instrument.

Sociological Synthesis

Accordingly, it becomes evident that cybersecurity and digital vulnerability constitute a complex social phenomenon in which the technical, cultural, and social dimensions intersect and cannot be understood apart from the societal structure and prevailing digital culture. Previous studies have demonstrated that the digital space is not simply an extension of technology but rather a direct extension of social relations, where pervasive cyber risks influence trust, interactions, and digital identity management.

Theoretical approaches likewise illustrate that digital security is an inseparable part of modern social risk management, whether in Beck's risk society, Goffman's symbolic interactionism, or Castells's network society.

It also becomes clear that digital vulnerability is not merely the result of technical weaknesses or individual errors but also the product of complex interactions among gaps in digital education, unequal access to technology, weak digital awareness, and ineffective institutional frameworks. This vulnerability directly affects social relationships within digital environments, as exposure to breaches and violations erodes trust, transforms interaction patterns, and redistributes power among different digital actors, whether individuals, organised groups, or technology companies.

Strategic Conclusions

The sociological analysis reveals that cybersecurity has become a strategic element in the stability of digital society, encompassing the protection of individuals, institutions, and network infrastructures. The development of a conscious digital culture, the enhancement of security awareness, and the activation of the role of social institutions such as the family, the school, and the media form the fundamental basis for reducing digital vulnerability.

Recent Algerian studies further confirm that the absence of strong cybersecurity governance within institutions increases the vulnerability of public digital services, compromising the stability of society as a whole.

From this perspective, cybersecurity may be understood as a comprehensive social phenomenon requiring integrated solutions that connect technology, policy, culture, and society. Building a stable and secure digital society demands multilayered strategies that include the following:

- ✓ strengthening digital culture,
- ✓ developing individuals' skills in protecting their digital identities,
- ✓ bridging technological gaps, and
- ✓ ensuring effective institutional governance of cybersecurity.

This research indicates that digital vulnerability is tied more closely to social structure and digital culture than to technology alone, and any attempt to address it without considering its social and cultural dimensions will be insufficient. It also shows that cybersecurity is not merely technical protection but also a fundamental social and

strategic factor reflecting a society’s capacity to organise itself, strengthen trust among its members, and preserve the stability of digital and institutional networks. Furthermore, the digital future of societies depends on integrating digital culture with social awareness and institutional policies to reduce risks, protect individuals and institutions, and ensure that the digital space is a safe and sustainable environment that supports social interactions and reinforces the stability of modern societies.

Conclusion

The study's findings demonstrate that threats in the digital space are no longer limited to data theft or cyberattacks; they now include direct social consequences, such as the erosion of trust among individuals, weak management of digital identity, and changes in patterns of digital social interaction. The study also revealed that gaps in digital education, unequal access to technology, and weak security awareness lead to varying levels of digital vulnerability across different social groups, rendering some groups more exposed to digital exploitation and extortion.

The analysis of the findings through theoretical approaches revealed that Beck's risk society framework clarifies how digital vulnerability emerges from socially produced risks that exceed individuals' ability to confront them. Moreover, Goffman's symbolic interactionism demonstrates that weak digital identity management leads to fragile social interactions. Castells's network society theory further illustrates that the structural complexity of digital networks expands the surface of vulnerability and redistributes power among different digital actors.

Previous studies, both Algerian and international, support this proposition, confirming that the absence of institutional governance and the weakness of digital culture increase society’s exposure to digital vulnerability and threaten its stability.

From this perspective, the significance of the research lies in linking technical analysis with social and cultural dimensions, allowing cybersecurity to be understood not merely as a technical protection tool but also as a fundamental pillar of social and digital stability. The study shows that managing digital vulnerability requires multidimensional strategies that involve individuals, institutions, and prevailing digital culture and that any response that fails to account for these dimensions will remain ineffective in the long term.

On the basis of the findings of this research, several recommendations can be proposed to increase cybersecurity and reduce digital vulnerability:

1. **Strengthening the digital prevention culture within society:**

   Community-based programs should be adopted to teach individuals how to interact safely in the digital space, with a focus on developing skills to detect misinformation and protect privacy.

2. **Development of digital support networks for the most vulnerable groups:**

   Platforms and support initiatives for vulnerable populations, such as women, children, and older adults, should be created to provide them with the tools and guidance needed for safe digital engagement.

3. **Encouraging collaboration between the public and private sectors:**

   Joint policies between government and technology institutions should be established to ensure the exchange of information on cyber risk and to develop rapid response plans for digital threats.

4. **Implementing periodic risk assessment mechanisms:**

   To develop tools for assessing cybersecurity risks at both the institutional and individual levels and to continuously identify and systematically address points of weakness.

5. **Enhancing applied and sociological research in digital security:**

   Scientific studies that integrate the technical and social dimensions should be conducted to develop comprehensive solutions that reduce digital vulnerability and strengthen the stability of the digital society.

6. **Integrating digital education into formal curricula:**

   Educational units on cybersecurity and digital culture in schools and universities should be added so that learners are equipped from an early age to deal with digital risks.

These recommendations emphasise that cybersecurity and digital vulnerability cannot be addressed solely through modern technologies but require a balanced interaction between individual awareness, societal culture, and institutional governance. The research also shows that any successful strategy must integrate technical knowledge with social and cultural understanding to ensure a safe and sustainable digital environment, strengthen trust within the digital society, and help build a more cohesive community capable of confronting emerging digital risks.

References:

Ali, N. (2003). *Arab culture and the information age*. Knowledge World Series, National Council for Culture, Arts and Letters.

Al-Hammadi, K. (2020). Cybersecurity awareness and its relationship to social behaviour across social media platforms. *Contemporary Social Studies Journal, 12*(3), 77–101.

Anderson, R. (2020). *Security engineering* (3rd ed.). Wiley.

Bada, M., & Nurse, J. R. C. (2019). The social and psychological impact of cyber-attacks. *arXiv*. https://arxiv.org/abs/1909.13256

Bauman, Z., & Lyon, D. (2013). *Liquid surveillance*. Polity Press.

Beck, U. (1992). *Risk society: Towards a new modernity*. Sage Publications.

Ben Barghouth, L. (2023). Cybersecurity and the protection of digital data privacy in Algeria in the era of digital transformation and artificial intelligence. *International Journal of Social Communication, 10*(1), 443–457.

Boyes, H. (2019). *Cybersecurity and cyber-resilience*. Springer.

Castells, M. (2010). *The rise of the network society* (2nd ed.). Wiley-Blackwell.

Cavelty, M. D. (2015). *Cybersecurity and threat politics: US efforts to secure the information age*. Routledge.

Charness, N., & Boot, W. R. (2009). Ageing and information technology use: Potential and barriers. *Current Directions in Psychological Science, 18*(5), 253–258.

Clarke, R., & Knake, R. (2010). *Cyber war: The next threat to national security and what to do about it*. Ecco.

Debray, R. (2017). *Le pouvoir et la vie numérique*. Gallimard.

Evans, M., Maglaras, L. A., He, Y., & Janicke, H. (2016). Human behaviour as an aspect of cybersecurity assurance. *arXiv*. https://arxiv.org/abs/1601.03921

Fuchs, C. (2014). *Social media: A critical introduction*. Sage Publications.

Goffman, E. (1959). *The presentation of self in everyday life*. Doubleday.

Kello, L. (2017). *The virtual weapon and international order*. Yale University Press.

Lévy, P. (1999). *Cyberculture*. Éditions Odile Jacob.

Lewis, J. (2018). *The cybersecurity dilemma: Hacking, trust, and fear between nations*. Rowman & Littlefield.

Livingstone, S., & Smith, P. K. (2014). Annual research review: Harms experienced by child users of online and mobile technologies. *Journal of Child Psychology and Psychiatry, 55*(6), 635–654.

Marwick, A., & Boyd, D. (2014). Networked privacy: How youth navigate online risks. *New Media & Society, 16*(7), 1051–1067.

Mansouri, H. (2022). New digital technologies for risk management in smart economic organisations. *Le Manager, 9*(2), 245–275. https://asjp.cerist.dz/en/article/205393

McKinsey & Company. (2024). *Cyberwar at the doorstep: Strategies for reducing emerging technology risks in financial services companies*.

Rainie, L., & Anderson, J. (2017). *The future of cybersecurity in the networked society*. Pew Research Centre.

Rainie, L., & Wellman, B. (2012). *Networked: The new social operating system*. MIT Press.

Ragnedda, M., & Muschert, G. W. (2013). *The digital divide: The internet and social inequality in an international perspective*. Routledge.

Reddy, G. N., & Ugander Reddy, G. J. (2014). A study of cyber security challenges and its emerging trends on digital society. *International Journal of Computer Science and Engineering*.

Ritzer, G. (2021). *The McDonaldization of society in the digital age*. Sage Publications.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.

Smith, A., & Duggan, M. (2019). *Cybersecurity and social risk in the digital era*. Pew Research Center.

Sorj, B. (2008). *Information societies and digital divides*. arXiv.

Van Dijck, J., & Poell, T. (2015). Understanding social media logic. In *Understanding social media*. Oxford University Press.

Whitman, M., & Mattord, H. (2022). *Principles of information security* (7th ed.). Cengage Learning.

Zamoura, J., & Ben Aissa, L. (2022). The importance of cybersecurity governance to ensure a secure digital transformation of public services in Algeria. *Advanced Economic Research Journal, 7*(2), 414–429.

Zawawi, L., & Ramli, F. (2023). Cyber threats and digital society security: A case study of Algeria. *Algerian Journal of Security and Development, 12*(2), 148–160.