SEPTEMBER 2025 (№35)
Volume 11; Issue 3; Page No. 117-131
ISSN: 2346-7916 (Print)
ISSN: 2587-5043 (Online)

INTERNATIONAL JOURNAL OF LAW: "LAW AND WORLD" www.lawandworld.ge

https://doi.org/10.36475/11.3.8

Cybersecurity in the Digital Era: Between Digital Transformation and Protection Challenges

Bouhafs Henen

PhD in Specialized Administrative Law, Faculty of Law, University of Aïn Témouchent, Algeria
Laboratory for markets, employment, legislation, and simulation in Maghreb countries
henen.bouhafs@univ-temouchent.edu.dz

ARTICLE INFO

Article History:

Received	16.05.2025
Accepted	18.08.2025
Published	30.09.2025

Keywords:

Cybersecurity, Digital transformation, Data protection, Cyberattacks

ABSTRACT

The enhancement of cybersecurity represents a cornerstone for the successful implementation of digital transformaion initiatives across various sectors. It plays a critical role in safeguarding digital systems against cyber threats and attacks that could disrupt operations and compromise continuity. As reliance on technology grows and smart systems become increasingly integrated into service delivery, the demand for a resilient and trustworthy cybersecurity infrastructure has become indispensable.

Cybersecurity serves as a fundamental enabler of trust in the integrity and confidentiality of data, protecting it from manipulation, breaches, or unauthorized disclosure. This, in turn, fosters a secure and transparent digital environment for information exchange, which enhances institutional performance and reduces operational costs arising from security breaches or technical failures.

The findings of this study indicate that nations and organizations possessing advanced cybersecurity capabilities — and investing proactively in emerging technologies — are more equipped to assert effective control over cyberspace. Such capacity ensures the realization of digital security and

strengthens national sovereignty. Cybersecurity thus emerges as a strategic instrument for digital defense and the protection of national interests at both domestic and international levels, positioning it as a vital element in achieving comprehensive and sustainable digital transformation.

INTRODUCTION

Contemporary society is situated at the core of the knowledge and information era, an era defined by the ubiquity of the web and pervasive networked communication, where the flow of information now surpasses any previously known form of exchange in human history. The transformations that characterize this phase represent a qualitative leap that far surpasses previous stages of human development, particularly in terms of scope, speed, capacity, and informational richness.

This evolving reality has shifted the world from geographical proximity to a condition of spatial convergence, transcending even Marshall McLuhan's seminal notion of a "global village". The unprecedented velocity and volume of information circulation have resulted in what is often termed the "information explosion", a phenomenon that carries profound positive and negative implications for the global community.

Simultaneously, this explosion has engendered a spectrum of security challenges of varying magnitude and impact, affecting both individuals and nation-states. These challenges increasingly necessitate intervention to protect sensitive information, especially that which pertains to national sovereignty and state security, within the framework of what is now understood as "cybersecurity".

In today's increasingly digital societies, information functions as a core axis across economic, political, and social dimensions, rendering it highly susceptible to threats and attacks. This underscores the urgent need to implement robust safeguards against cybercrime in its many forms. The imperative becomes all the more acute as information continues to serve as a primary source of both wealth and intellectual capital.

The deepening interconnectivity among institutions worldwide compounds the risk: a single breach within one entity's digital infrastructure can rapidly cascade into broader systemic vulnerabilities due to the intricate web of informational dependencies that now characterize global institutional operations.

Moreover, cyberattacks have evolved into a formidable instrument within the landscape of international competition, particularly in the economic domain, where such attacks may serve espionage or sabotage functions between states. The severity of these threats escalates dramatically when critical infrastructure is targeted, as such incidents have the potential to trigger geopolitical conflict, especially in already volatile regions.

Consequently, cyberattacks now pose a direct threat to regional and global peace and security. These dynamics make it increasingly necessary to recognize cybersecurity not merely as a technical concern but as a strategic imperative, an essential dimension of national security and a cornerstone of any comprehensive digital transformation agenda. Given the strategic significance and high-stakes nature of cybersecurity risks, an increasing number of nations are integrating cybersecurity measures into their overarching national security doctrines.

In light of the foregoing, this study is guided by the following research question: **Is there a measurable correlation between the various dimensions of digital transformation**

and the level of cybersecurity implemented within institutional frameworks? Furthermore, to what extent does digital transformation contribute to reinforcing, or potentially undermining, cybersecurity?

To address this question, the research adopts an inductive approach, beginning with partial observations and analyses of real-world and contemporary cases associated with digital transformation and its implications for cybersecurity. This includes the monitoring of incidents such as cyberattacks targeting critical infrastructure, data breaches, and the implementation of modern protective strategies by specific countries and institutions. Additionally, the analytical method is applied to examine these incidents and discern the nature of the relationship between digital transformation and the increasing necessity for cybersecurity.

METHODOLOGY

This research is based on a doctrinal-analytical approach, which involves the examination of international and national legal documents, strategic frameworks, and policy acts. A comparative legal method has also been employed, entailing a systematic comparison of models from different jurisdictions. In addition, the study integrates a case study approach, focusing on detailed discussions of specific examples of legal practice. The research materials include: normative acts and official documents (international conventions, EU directives, U.S. federal standards, Algerian national legislation); reports of international organizations (current publications of ENISA, NIST, and other institutions); academic literature (scholarly works published over the past decade reflecting contemporary trends in digital transformation and cybersecurity); and practical cases (decisions of international courts and real-life cyberattack examples illustrating the issues under examination). The article relies primarily on normative and documentary sources. Quantitative analysis, including modeling or statistical processing of cybersecurity indices, does not fall within the scope of this study; however, this direction is identified as a perspective for future research.

1. DIGITAL TRANSFORMATION AS A CATALYST FOR THE EVOLUTION OF CYBERSECURITY

Amid the rapid proliferation of digital technologies and the growing dependence of institutions on intelligent solutions across a wide array of sectors, digital transformation has emerged as a foundational force in reshaping the landscape of work environments and service delivery.

Parallel to this transformation is the escalating urgency to safeguard data and protect digital infrastructure from a surge in cyber threats, rendering cybersecurity a critical and continuously evolving domain. Within this context, digital transformation can be seen not only as a driver of innovation and operational efficiency but also as a catalyst for the advancement of cybersecurity mechanisms and methodologies. These advances align with the increasing complexity of digital threats and the elevated expectations placed on institutions to secure information effectively.

1.1. Digital transformation and the variables of the digital age

Contemporary global dynamics are characterized by transformative changes spurred by the digital revolution, which has redefined economic, social, educational, and security paradigms. With the relentless acceleration of technological innovation, digital transformation has shifted from being a strategic option to becoming an imperative, imposed by the defining variables of the digital era, including artificial intelligence, big data analytics, and the Internet of Things.

These technological variables do not merely influence the nature of services and infrastructure; they also reshape fundamental notions of operational efficiency, responsiveness, and communicative interaction. As a result, both individuals and institutions are compelled to embrace innovative digital frameworks capable of adapting to the pace and demands of this transformation.

1.1.1. The concept of digital transformation

The current era is marked by an intensifying digital transformation, which has established itself as a global trend permeating all domains due to persistent technological advancement. This transformation has redefined how efficiency and effectiveness are conceptualized within institutional structures and has led to the emergence of new perspectives concerning institutional performance and excellence.

As a result, adopting digitalization has become a strategic imperative, one that enables the initiation of systemic change and the pursuit of excellence across a range of sectors. Consequently, the discussion must address the concept of digital transformation by first providing its definitions and then exploring its core dimensions.

1.1.1.1. Definition of digital transformation

Digital transformation is defined as: *"A modern business model that utilizes digital technologies to develop innovative products and services, as well as the methods through which they are delivered, with an emphasis on addressing the needs of customers or end users".*[1]

It is further defined as: *"The process of integrating digital technologies into business operations, resulting in a radical and comprehensive transformation in the way value is created and delivered to the end user, while simultaneously reflecting a cultural shift that institutions must adapt to".*

In a similar vein, it is described as: *"Innovation driven by a comprehensive transformation process that incorporates existing digital technologies into methods for generating value, conducting production, and managing business operations, particularly by redefining the underlying thought processes".*[2]

Accordingly, digital transformation can be defined as a comprehensive and strategic process aimed at the systematic integration of digital technologies across all facets of institutional operations. Its purpose is to foster the innovation of new products and services, refine the mechanisms through which value is delivered to the end user, and instigate cultural and organizational transformation. This process compels institutions to fundamentally reconsider their business models, leadership methodologies, and cognitive frameworks to align with the complex and evolving demands of the digital age.

1.1.1.2. Dimensions of digital transformation

Digital transformation represents a multifaceted phenomenon, within which two principal dimensions are particularly prominent:[3]

1.1.1.2.1. Digital technologies

At its core, digital transformation is driven by ongoing advancements in digital technologies. Scholarly literature consistently identifies three primary technologies as central to institutional digital transformation: the Internet, digital analytics, and cloud computing. These technologies are interrelated and have witnessed exceptional development in recent years. Their combined capabilities have enabled institutions to restructure and optimize their internal processes and service delivery in a digitally integrated and comprehensive manner.

1 Slaimi, D., Bouchi, Y. (2019). Digital transformation between necessity and risks. Journal of Legal and Political Sciences (2), Algeria.

2 Ferhane, F. (2017). The skills and core capabilities essential to the success of digital transformation in enterprises. Revue des Sciences Économiques, 13(15), p. 52.

3 Henriette, E., Feki, M., Boughzala, I. (2016). Digital transformation challenges. Mediterranean Conference on Information Systems (MCIS). AIS Electronic Library (AISeL), p. 3.

1.1.1.2.2. User experience

Digital transformation places the end user, be it a consumer or an employee, at the center of institutional priorities. Contemporary users increasingly demand superior quality, enhanced flexibility, and personalized engagement in the products and services they consume. They also expect immediate, context-aware responses to their shifting needs. This reality is especially pronounced among digital-native generations, who display heightened technological literacy and a pronounced inclination to share their experiences through social media platforms.

To accommodate these continually evolving expectations, institutions must reassess their operational behaviors and adopt marketing strategies that resonate with contemporary consumption patterns. Consequently, digital transformation often initiates with a reconfiguration of marketing functions through the deployment of advanced customer relationship management (CRM) tools. These systems are progressively integrated with social network analysis functionalities to enrich the interactive and participatory aspects of customer engagement.

This transformative impact extends further to human resource management, particularly through the utilization of employee relationship management (ERM) systems. Within this framework, employees are perceived as "internal customers", and significant efforts are directed toward delivering a workplace experience that mirrors the standard of service extended to external clients.

1.1.2. Requirements of digital transformation

The implementation of digital transformation spans several domains, notably technology, data, and human capital. These requirements are outlined in greater detail below:

1.1.2.1. Technologies

Digital transformation is predicated on a cohesive and sophisticated technological ecosystem encompassing hardware, data repositories, storage infrastructures, and software platforms, all of which function within advanced IT environments and data centers designed to guarantee both high performance and operational continuity. This ecosystem must be capable of delivering consistent service quality that satisfies the expectations of the organization's personnel, clients, and external partners.

To ensure these outcomes, it is essential to deploy specialized technical teams tasked with overseeing and maintaining the technological infrastructure and communication networks with precision, dependability, and efficiency.

1.1.2.2. Data

Business organizations must engage in consistent and effective data management and analysis to ensure the availability of qualitative, reliable, and comprehensive information. This requires the implementation of advanced statistical analysis tools and the development of predictive capabilities that assist in shaping future strategic orientations. Continuous monitoring of data flows, coupled with their optimal utilization, is essential for achieving institutional objectives and realizing broader strategic goals.[4]

1.1.2.3. Human resources

Human resources constitute a fundamental pillar in advancing digital transformation, as they represent one of the most critical assets for confronting the complex challenges and pressures that institutions currently face. These resources serve as a driving force for progress and development across various sectors.

Nonetheless, many countries, particularly those in the developing world, grapple with substantial obstacles stemming from the scarcity of skilled professionals equipped to navigate and adapt to the demands of the digital environment. This deficiency poses a significant barrier to the integration of advanced technologies and the effective implementation of digital transformation initiatives.

4 Chaouchi, K., Khellouf, Z. (2023). Digital transformation in Algeria. Journal of Accounting, Auditing, and Finance (01), Algeria.

Therefore, there is a pressing need to formulate strategic plans aimed at cultivating and enhancing human capacities. This includes attracting new talent with a deep understanding of the digital transformation landscape and leveraging existing technological resources to support institutional advancement in this domain.

1.2. The evolution of cybersecurity in response to digital transformation

In tandem with the accelerating momentum of digital transformation and the growing institutional dependence on intelligent systems and digital platforms, the protection of data and digital systems has assumed critical importance. This evolving reality has given rise to a complex threat landscape that demands sophisticated security solutions capable of addressing the emerging risks within cyberspace.

As a direct outcome of this transformation, the cybersecurity field has undergone notable expansion, particularly in the development of new tools and strategic approaches. Increasingly, cybersecurity operations rely on artificial intelligence, data analytics, and machine learning to anticipate, detect, and neutralize potential cyberattacks. Consequently, digital transformation has not only introduced novel security challenges but has simultaneously driven the evolution and enhancement of cybersecurity capabilities.

1.2.1. The concept of cybersecurity

This section outlines the concept of cybersecurity by presenting its definitions and identifying its principal dimensions.

1.2.1.1. Definition of cybersecurity

Cybersecurity is a relatively modern concept, first introduced in the United States during the late 1980s. However, it did not attain widespread recognition and application until the early 2000s, coinciding with the rapid acceleration of technological development and the parallel escalation of cyber threats and vulnerabilities, which have since emerged as significant global security concerns.

Cybersecurity is defined as: *"A set of technical and administrative measures used to prevent unauthorized access to computer networks or to prevent their misuse, in addition to the recovery of the electronic information they contain, with the aim of ensuring the continuous operation of information systems and safeguarding the security, confidentiality, and privacy of data for actors within cyberspace".*[5]

The American Institute of Certified Public Accountants (AICPA) defined cybersecurity as: "a set of practices and procedures designed to protect data and information from cyber threats".[6] The American Institute of Certified Public Accountants (AICPA) has established a comprehensive set of cybersecurity standards for the accounting profession, including the Statements on Standards for Accounting and Review Services (SSARS) and the Trust Services Principles and Review Services. These frameworks are intended to assist accountants in safeguarding the digital business environment through the implementation of effective data security and privacy controls, thereby reinforcing confidence in the systems and processes underpinning the delivery of professional services.[7] Conversely, the National Institute of

5 Bougrara, Y. (2018). Cybersecurity: The Algerian strategy for security and defense in cyberspace. African and Nile Basin Studies Journal (3), Democratic Center, Berlin.

6 Daoud, M. M., Serag, A. A. (2022). A proposed Framework for Studying the Impact of Cybersecurity on Accounting Information to Increase Trust in The Financial Reports in the Context of Industry 4.0: An Event, Impact and Response Approach. Trade and Finance, 42(1).

7 Through these standards, the American Institute of Certified Public Accountants (AICPA) seeks to assist organizations in protecting their data and ensuring business continuity. These standards include: 1. Risk Assessment: Identifying potential threats and evaluating the risks associated with systems and data; 2. Access Control:Regulating who can access sensitive information and how it is used; 3. Encryption: Apply-

Standards and Technology (NIST, 2024) has adopted the Cybersecurity Framework (CSF 2.0) as a key international reference for the development of protection strategies and the management of risks at the institutional level.[8]

The Securities and Exchange Commission (SEC) has defined cybersecurity as the protection of systems, networks, and digital data from cyberattacks and unauthorized access. In other words, the SEC addresses cybersecurity in the context of safeguarding sensitive information belonging to investors and registered companies.[9]

As such, cybersecurity encompasses a domain dedicated to formulating procedures and adopting standards and protective measures to address threats, prevent security breaches, and reduce the potential impact of such incidents to the lowest possible level, even in worst-case scenarios.

From an operational perspective, cybersecurity can be summarized through the following key elements:

1. Cybersecurity comprises a collection of defensive tools and mechanisms designed to detect intrusions and prevent unauthorized access;
2. It includes the safeguarding of computer networks and their associated data from infiltration, malicious tampering, or disruption attempts;
3. Cybersecurity involves the mitigation of risks posed by malicious attacks on software, hardware, and networks. This includes tools for intrusion detection, virus mitigation and removal, the application of authentication protocols, and the activation of secure, encrypted communications;[10]
4. More broadly, cybersecurity is understood as an ensemble of practices and technologies developed to defend systems, networks, and software infrastructure against all forms of digital attack, whether originating from hacking attempts, malware infections, or other cyber threats targeting the integrity of information and digital assets.

1.2.1.2. Foundations of cybersecurity

In a digital world where dependence on technology is continuously growing, cybersecurity has become an indispensable necessity for safeguarding data and systems against cyberattacks. Recognizing the true significance of cybersecurity is critical at both the individual and institutional levels. In general, cybersecurity is centered on three primary objectives:

1.2.1.2.1. Confidentiality

- ***Protection of personal data and sensitive information***: Cybersecurity offers effective mechanisms to control access to data, ensuring that only authorized individuals or entities can retrieve or manipulate it. This is essential for protecting personal data such as names, addresses, and financial records, as well as sensitive institutional information, including patents and proprietary designs.
- ***Prevention of data theft and fraud***: Cybersecurity plays a pivotal role in preventing attempts by intruders to steal data, thereby substantially lowering the risks of fraud and identity theft.

ing cryptographic methods to safeguard data during storage and transmission; 4. Awareness and Training: Educating employees on cybersecurity best practices and how to recognize potential attacks; 5. Incident Response: Establishing plans for a rapid and effective response in the event of a security breach.

8 NIST. (2024). Fiscal Year 2024 Annual Report on Cybersecurity and Privacy Program (SP 800-236). National Institute of Standards and Technology. Available at: <https://www.nist.gov/publications/fiscal-year-2024-annual-report-nist-cybersecurity-and-privacy-program>.

9 Rahmawati, M. L., Sukoharsono, E. G., Rahman, A. F., Prihatiningtias, Y. W. (2023, June). Demistifying of Triple-Entry Accounting (TEA): Integrating the Block Economics Education, In Ninth Padang International Conference on Economics, Business and Management, Accounting and Entrepreneurship (PICEEBA 2022), Atlantis Press, pp. 23-31.

10 Bara, S. (2017). Cybersecurity in Algeria: Institutions and policies. Algerian Journal of Human Security, (04), Algeria.

1.2.1.2.2. Integrity

- ***Ensuring data accuracy and completeness*:** Cybersecurity safeguards the integrity of data by preventing unauthorized alterations or damage. This function is vital for maintaining the precision and reliability of data, which directly influences operational effectiveness and the soundness of decision-making processes.
- ***Protection from destructive attacks*:** Cybersecurity counters malicious activities aimed at damaging or corrupting data, thereby preserving information reliability and supporting the continuity of business operations.

1.2.1.2.3. Availability

- ***Ensuring business and service continuity*:** Cybersecurity ensures the constant availability of systems, services, and information, thus enabling uninterrupted business functions and service delivery.
- ***Avoidance of financial losses*:** By ensuring consistent access to digital resources, cybersecurity helps minimize potential financial damages associated with service downtime or data loss.[11]

1.2.1.3. Cybersecurity legal framework

The Budapest Convention on Cybercrime (2001) is regarded as the first binding international instrument aimed at harmonizing national legislations, developing advanced investigative techniques, and enhancing international cooperation in combating cybercrime. It explicitly criminalizes acts such as illegal access to systems, data interference, system interference, and computer-related fraud, while also establishing detailed mechanisms for mutual legal assistance among member states.

In contrast, the Algerian legislator has gradually incorporated provisions related to cybersecurity within its legal framework. Law No. 04-15[12] of 2004 and Law No. 06-23[13] of 2006 amended the Penal Code to criminalize illegal access, modification, deletion, or destruction of data. Furthermore, Law No. 09-04[14] of 2009 introduced specific rules for the prevention and combating of offenses related to information and communication technologies, including measures such as electronic surveillance, cooperation with service providers, and the exchange of international judicial assistance.

Despite these efforts, Algerian legislation remains less comprehensive compared to the Budapest Convention, particularly regarding the harmonization of cybercrime definitions, the expansion of procedural powers for digital investigations, and the establishment of structured mechanisms for international cooperation.

Accordingly, aligning Algerian legislation with the standards set forth in the Budapest Convention would significantly enhance its effectiveness in addressing cross-border cyber threats and strengthen its capacity for international collaboration in this critical field.

Practical case study: Microsoft v. United States (2016)

In 2013, a U.S. federal court issued a warrant to Microsoft under the Stored Communications Act (SCA) compelling the company to disclose the contents of an email account belonging to a suspect in a narcotics trafficking case. While Microsoft provided the non-content data stored within the United States, it refused to release the email content stored on its servers in Dublin, Ireland, arguing that U.S. warrants could not extend beyond national borders. The government, on the other hand, insisted that Microsoft

11 Hamidi, H., Taileb, N. (2022). A conceptual introduction to cybersecurity. Madar Journal for Digital Communication Studies (Issue unspecified), Algeria.

12 People's Democratic Republic of Algeria. (2015). Law No. 15-04 of 11 Rabi' al-Thani 1436 AH establishing the general rules relating to electronic signature and certification (Official Gazette, No. 6).

13 Ibid. (2006). Law No. 06-23 of 29 Dhu al-Qi'dah 1427 AH amending and supplementing Ordinance No. 66-156 of 18 Safar 1386 AH (June 8, 1966) relating to the Penal Code (Official Gazette, No. 84).

14 Ibid. (2009). Law No. 09-04 of 14 Sha'ban 1430 AH containing the specific rules for the prevention of crimes related to information and communication technologies and their combating (Official Gazette, No. 43).

retained control over the data regardless of its physical location. After prolonged litigation, the Court of Appeals for the Second Circuit ruled in July 2016 that the SCA does not authorize U.S. courts to issue warrants for data stored abroad, thereby overturning the lower court's decision and vacating the contempt order against Microsoft.[15]

In conclusion, the judgment affirmed that U.S. warrants are territorially limited and cannot be applied to data stored overseas. This outcome reinforced the principle of data sovereignty and highlighted the pressing need for coherent international legal frameworks, such as the Budapest Convention, to effectively address cross-border cybercrime.

1.2.2. Cybersecurity requirements in the context of digital transformation

In light of ongoing technological advancements and the acceleration of digital transformation, cybersecurity has become one of the most critical and urgent concerns. It functions as the primary defense mechanism for protecting digital systems and networks, with the core objective of securing sensitive data and information from unauthorized access and potential cyber threats.

Ensuring effective cybersecurity necessitates the adoption of comprehensive, multi-layered strategies encompassing prevention, real-time monitoring, and robust threat response mechanisms. These include the deployment of advanced technologies such as encryption and software-based defense systems, along with the promotion of digital security awareness through user education and training on best practices.

A major challenge confronting the field lies in the ever-evolving nature of cyber threats. Malicious actors continuously seek innovative techniques to breach digital infrastructures. As a result, cybersecurity specialists must remain informed about the latest developments and threat vectors to effectively counter these risks.

Despite the complexity of these challenges, robust cybersecurity can be achieved through strategic investment in modern technologies, widespread promotion of digital security awareness, and reinforced cooperation between institutions and relevant governmental authorities.

Thus, cybersecurity constitutes a shared responsibility involving individuals, organizations, and state institutions. Heightened awareness and collaborative action form the essential foundation for protecting and securing digital ecosystems.

2. CYBER CHALLENGES IN THE DIGITAL ERA AND RESPONSE STRATEGIES

In light of the massive expansion in the use of digital technology, cyberspaces have become arenas for increasing challenges that threaten the security of individuals, institutions, and states alike. The digital age, despite its advantages in terms of speed and information exchange, has simultaneously generated new forms of complex and advanced cyberattacks, ranging from data theft and cyber extortion to threats targeting critical infrastructure.

In the face of these growing challenges, it has become imperative to adopt comprehensive and flexible cybersecurity strategies that combine technical, human, and organizational dimensions to ensure business continuity and protect sensitive information from any potential breach.

2.1. Key cyber threats in the digital age

With the growing reliance on digital systems and the expansion of IT infrastructure, advanced cyber threats have emerged that align with the nature of the digital era. These threats have become a growing concern for both institutions and governments, making it essential to identify the most prominent ones and analyze

15 Microsoft v. United States, No. 14-2985 (2d Cir. 2016).

their impact within the context of accelerating digital transformation.

2.1.1. Cyberattacks

Cyberattacks are among the most significant challenges facing cybersecurity, as they can lead to the leakage of sensitive information and financial data, causing severe damage to governmental institutions, companies, and even individuals. Addressing these threats requires strengthening protection against cybercrimes by securing computer systems and networks against malicious attacks, including viruses, malware, ransomware, and denial-of-service (DoS) attacks.[16]

In this regard, the European Union Agency for Cybersecurity (ENISA, 2024) underscores that ransomware and supply chain attacks constitute some of the most severe threats confronting states and organizations in the digital era.[17]

2.1.2. Phishing

This involves attempts to deceive users into providing sensitive data, such as passwords or bank card information, often through fake email messages.

2.1.3. Social engineering

Social engineering is one of the techniques employed by cybercriminals, who impersonate influential individuals to deceive the victim and manipulate them into revealing sensitive information that serves specific purposes. This often includes requests for financial payments or access to confidential data. Attackers use various tools to breach computers and gain unauthorized access to service providers, enabling them to steal credit card numbers, passwords, and other personal information from network users.[18]

2.1.4. Attacks on the Internet of Things (IoT)

The Internet of Things (IoT) is considered an emerging technology that connects billions of computing devices to the Internet. Sensors and computing devices communicate through Internet protocols to exchange information and share data.[19]

IoT devices face several security risks due to their vulnerabilities:

- Device weaknesses: IoT devices are designed with limited processors and memory, making them susceptible to vulnerabilities. Weak default configurations, outdated software, and a lack of security updates make these devices ideal targets for attacks;
- Data privacy: IoT devices collect massive amounts of sensitive data, including personal information. Insecure storage, weak encryption, or poor data management can lead to unauthorized access;[20]
- Network security: Devices rely on wireless protocols such as Wi-Fi, Bluetooth, and cellular networks. Attackers may target these channels for eavesdropping or data tampering. Insecure configurations and weak encryption compromise network security.[21]

16 Manasra, Y. (2023). Reconciling internet governance and state cybersecurity. Voice of Law Journal (2), Algeria.

17 ENISA. (2024). ENISA Threat Landscape 2024. European Union Agency for Cybersecurity. Available at: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024>.

18 Hamidi, H., Taileb, N. (2022). A conceptual introduction to cybersecurity. Madar Journal for Digital Communication Studies (Issue unspecified), Algeria.

19 Gunduz, M. Z., Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. Computer Networks, 169, 107094. Available at: <https://doi.org/10.1016/j.comnet.2019.107094](https://doi.org/10.1016/j.comnet.2019.107094)>.

20 Admass, W. S., Munaye, Y. Y., Diro, A. A. (2024). Cyber security: State of the art, challenges and future directions. Cyber Security and Applications, 2, 100031, p. 5. Available at: <https://doi.org/10.1016/j.csa.2024.100031](https://doi.org/10.1016/j.csa.2024.100031>.

21 AsSadhan, B., Moura, J. M. F. (2014). An efficient method to detect periodic behavior in botnet traffic by analyzing control plane traffic. Journal of Advanced Research, 5 (4), pp. 435–448. Available at: <https://doi.org/10.1016/j.jare.2013.11.005>; <https://doi.org/10.1016/j.jare.2013.11.005>.

2.1.5. Cloud computing

The increasing reliance on cloud computing services exposes organizations to new risks such as data breaches, unauthorized access, insecure APIs, and shared infrastructures, which can lead to data loss and disruption of critical services.[22]

2.2. Protection and response strategies against digital threats

Amid the escalating cyber threats and the continuous evolution of attack techniques, the adoption of effective strategies has become imperative for safeguarding digital infrastructure, securing information, and ensuring the continuity of business operations. The most prominent among these strategies include:

2.2.1. Enhancing security awareness

Fostering a cybersecurity-oriented culture among all users within institutions through continuous training sessions and workshops is essential. These initiatives focus on raising awareness regarding the identification of phishing attacks, social engineering tactics, and malware threats.

2.2.2. Regularly updating systems and software

Routine security updates constitute a primary defense mechanism against vulnerabilities that may be exploited by malicious actors. The implementation of patch management systems is necessary to ensure that software remains consistently updated and resilient against known threats.

2.2.3. Using advanced protection tools

It is crucial to deploy integrated security solutions that encompass firewalls, antivirus programs, intrusion detection and prevention systems (IDS/IPS), and robust encryption protocols to safeguard data during both transmission and storage.

2.2.4. Implementing access control policies

Access to sensitive information must be restricted based on the principle of "least privilege", with strong enforcement of user authentication procedures through multi-factor authentication systems.

2.2.5. Backup and emergency response

The establishment of a comprehensive data recovery and emergency response strategy is vital. This should include routine data backup processes and the execution of simulated cyberattack exercises to assess readiness and ensure swift response capabilities.

2.2.6. System monitoring and log analysis

The use of network monitoring tools and log analysis facilitates the detection of abnormal activities and supports the early identification of potential intrusion attempts.

2.2.7. Compliance with standards and regulations

Adherence to international security standards and regulatory frameworks such as ISO/IEC 27001 and the General Data Protection Regulation (GDPR) significantly enhances the overall security posture and reduces legal and compliance-related risks.

2.2.8. Behavior-based security

This approach involves the detection of threats by monitoring and analyzing communication patterns between users and devices on a network. Any deviation from established behav-

22 Thakur, K., Qiu, M., Gai, K., Ali, M. L. (2016). An investigation on cyber security threats and security models. InProceedings of the 2nd IEEE International Conference on Cyber Security and Cloud Computing (CSCloud 2015) – IEEE International Symposium on Smart Cloud, IEEE, pp. 307-311. Available at: <https://doi.org/10.1109/CSCloud.2015.71>; <https://doi.org/10.1109/CSCloud.2015.71>.

ioral norms is flagged as an anomaly, potentially signaling the presence of an attack in progress.

NetFlow technology

NetFlow is employed to gather metadata on network traffic, including information about users, devices, and communication flows. This data is instrumental in identifying and analyzing irregular network behavior indicative of security threats.

Penetration testing (also known as Pen Testing)

Penetration testing involves evaluating security vulnerabilities in systems and networks by simulating attacks. Testers attempt to exploit identified weaknesses, and the findings are used to strengthen system defenses and improve security effectiveness.

While institutions dedicate significant efforts to prevent cybersecurity breaches, no security system can guarantee absolute protection. Therefore, maintaining continuous threat awareness and persistently evolving protection strategies remains an essential component of comprehensive cybersecurity management.

The following table illustrates the impact of different digital transformation models on cybersecurity and how they address threats (**see Table 1, 2**).

Digital Transformation Models

In fact, digital transformation enhances cybersecurity management by improving threat monitoring, response, and data analysis, but it also increases complexity and poses significant challenges for data protection and privacy.

CONCLUSION

The world has witnessed remarkable technological progress, particularly in the domain of information and communication technologies. This progress has led to an unprecedented expansion of the digital sphere, reflected in the vast and diverse range of content and services now accessible via the internet, from artificial intelligence and the Internet of Things to virtual and augmented reality and cloud computing.

While these advancements have delivered immense benefits, they have also introduced serious challenges and risks, most notably the rise of increasingly sophisticated cyber threats. These include the spread of malicious viruses, data breaches, espionage operations, and even the destruction of digital infrastructure. In certain instances, such attacks have evolved to the extent that they now pose direct threats to national security, falling under the scope of what is now recognized as cyber warfare.

In light of this complex and evolving landscape, there is a pressing need to adopt both defensive and offensive cybersecurity strategies that incorporate advanced security technologies and go beyond the limitations of conventional territorial boundaries.

Cyberspace has transformed from a purely technological realm into an open and contested arena where the security of nation-states can be targeted and compromised with alarming ease. As a result, states are increasingly focused on developing comprehensive cybersecurity systems, including tools for surveillance, deterrence, and response, with the ultimate aim of securing their data and protecting their critical national interests.

Based on the preceding analysis, the following conclusions can be drawn:

- Cyberspace has introduced multifaceted and far-reaching challenges affecting all nations without exception. It has also played a pivotal role in redefining global power dynamics according to new criteria that transcend traditional frameworks;
- This domain has produced intensifying threats, compelling nations to urgently adopt robust national cybersecurity strategies, particularly in light of mounting global challenges;
- The increasing prevalence of cyberattacks, espionage activities, and recurring

electronic intrusions has necessitated a reexamination of the concept of absolute sovereignty, which has become vulnerable to digital exposure and penetration, ultimately threatening national stability and security.

In light of these findings, the following recommendations are proposed:

- It is essential to invest in the development of secure digital infrastructure that aligns with the pace of digital transformation, while allocating sufficient material and human resources to support cybersecurity operations;
- Governments and institutions should establish well-defined strategic plans that encompass binding policies, protocols, and legislative frameworks to address the intensifying digital threat landscape;
- Public awareness campaigns and continuous training initiatives should be launched to educate users across all sectors on cyber risks and preventive measures;
- Educational and training programs should be strengthened to prepare skilled national professionals in the field of cybersecurity, with particular attention to modern technological competencies;
- Artificial intelligence solutions, machine learning models, and big data analytics should be adopted to enhance threat detection capabilities and ensure rapid response to emerging risks;
- Dedicated units should be established to monitor digital networks and manage cyber incidents with professionalism and speed;
- Cooperation should be encouraged between institutions at both national and international levels to facilitate the exchange of information and expertise related to cyber threats and security strategies;
- Cybersecurity must be understood not as a standalone component, but as an integral and indispensable element of digital transformation efforts, ensuring the long-term success and resilience of digital initiatives.

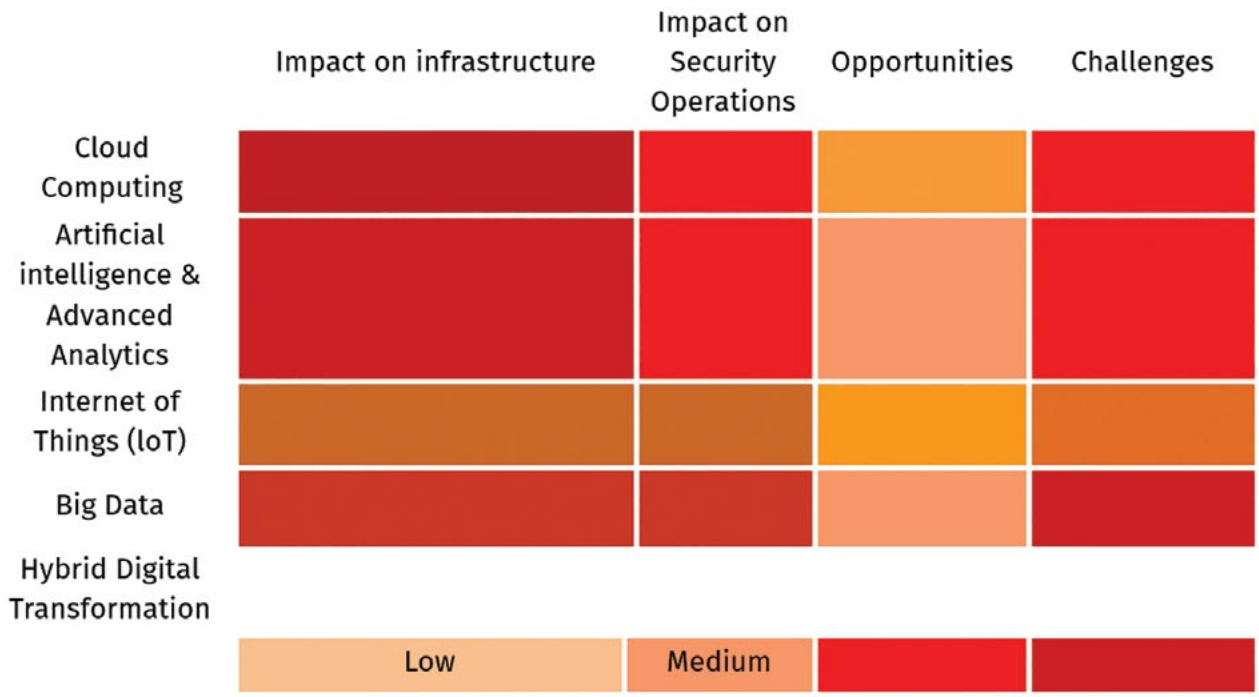
APPENDIX

TABLE 1. Impact of Digital Transformation Models on Cybersecurity

DIGITAL TRANSFORMATION MODEL	IMPACT ON INFRASTRUCTURE	IMPACT ON SECURITY OPERATIONS	OPPORTUNITIES	CHALLENGES	CYBERSECURITY IMPACT LEVEL
Cloud Computing	Centralized and Scalable Data Storage	Enhanced Update and Backup Management	Flexible Data Access and Capability Expansion	Risks of Data Breaches and Unauthorized Access	High
Artificial Intelligence and Advanced Analytics	Advanced Network and Systems Monitoring	Early Threat Detection and Behavior Analysis	Improved Attack Response and Reduced Human Errors	AI-Driven Attacks and Data Biases	High
Internet of Things (IoT)	Connectivity of Smart Devices to the Internet	Device Monitoring and Activity Logging	Mass Data Collection for Performance Analysis	Weak Device Security and Privacy Threats	Medium
Big Data	Storage and Analysis of Large Volumes of Data	Threat and Attack Pattern Analysis	Supporting Data-Driven Security Decision-Making	Challenges in Privacy Protection and Sensitive Data Storage	High

Hybrid Digital Transformation	Hybrid of On-Premises and Cloud Systems	Integration of Traditional Security Systems with Automation	Enhancing Flexibility and Threat Adaptation	Complexity in Management and Coordination of Security Policies	Medium

TABLE 2. Digital Transformation Models



REFERENCES

Scientific literature and conference papers:

Admass, W. S., Munaye, Y. Y., Diro, A. A. (2024). Cyber security: State of the art, challenges and future directions. Cyber Security and Applications, 2, 100031.s Available at: <https://doi.org/10.1016/j.csa.2024.100031](https://doi.org/10.1016/j.csa.2024.100031>.

AsSadhan, B., Moura, J. M. F. (2014). An efficient method to detect periodic behavior in botnet traffic by analyzing control plane traffic. Journal of Advanced Research, 5 (4). Available at: <https://doi.org/10.1016/j.jare.2013.11.005>; <https://doi.org/10.1016/j.jare.2013.11.005>.

Bara, S. (2017). Cybersecurity in Algeria: Institutions and policies. Algerian Journal of Human Security, (04), Algeria.

Bougrara, Y. (2018). Cybersecurity: The Algerian strategy for security and defense in cyberspace. African and Nile Basin Studies Journal (3), Democratic Center, Berlin.

Chaouchi, K., Khellouf, Z. (2023). Digital transformation in Algeria. Journal of Accounting, Auditing, and Finance (01), Algeria.

Daoud, M. M., Serag, A. A. (2022). A proposed Framework for Studying the Impact of Cybersecurity on Accounting Information to Increase Trust in The Financial Reports in the Context of Industry 4.0: An Event, Impact and Response Approach. Trade and Finance, 42(1).

Ferhane, F. (2017). The skills and core capabilities essential to the success of digital transformation in enterprises. Revue des Sciences Économiques, 13(15).

Gunduz, M. Z., Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. Computer Networks, 169, 107094. Available at: <https://doi.org/10.1016/j.comnet.2019.107094](https://doi.org/10.1016/j.comnet.2019.107094)>.

Hamidi, H., Taileb, N. (2022). A conceptual introduction to cybersecurity. Madar Journal for Digital Communication Studies (Issue unspecified), Algeria.

Henriette, E., Feki, M., Boughzala, I. (2016). Digital transformation challenges. Mediterranean Conference on Information Systems (MCIS). AIS Electronic Library (AISeL).

Manasra, Y. (2023). Reconciling internet governance and state cybersecurity. Voice of Law Journal (2), Algeria.

Rahmawati, M. L., Sukoharsono, E. G., Rahman, A. F., Prihatiningtias, Y. W. (2023, June). Demistifying of Triple-Entry Accounting (TEA): Integrating the Block Economics Education, In Ninth Padang International Conference on Economics, Business and Management, Accounting and Entrepreneurship (PICEEBA 2022), Atlantis Press.

Slaimi, D., Bouchi, Y. (2019). Digital transformation between necessity and risks. Journal of Legal and Political Sciences (2), Algeria.

Thakur, K., Qiu, M., Gai, K., Ali, M. L. (2016). An investigation on cyber security threats and security models. InProceedings of the 2nd IEEE International Conference on Cyber Security and Cloud Computing (CSCloud 2015) – IEEE International Symposium on Smart Cloud, IEEE. Available at: <https://doi.org/10.1109/CSCloud.2015.71>; <https://doi.org/10.1109/CSCloud.2015.71>.

Reports:

ENISA. (2024). ENISA Threat Landscape 2024. European Union Agency for Cybersecurity. Available at: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024>.

NIST. (2024). Fiscal Year 2024 Annual Report on Cybersecurity and Privacy Program (SP 800-236). National Institute of Standards and Technology. Available at: <https://www.nist.gov/publications/fiscal-year-2024-annual-report-nist-cybersecurity-and-privacy-program>.

Legal acts:

People's Democratic Republic of Algeria. (2006). Law No. 06-23 of 29 Dhu al-Qi'dah 1427 AH amending and supplementing Ordinance No. 66-156 of 18 Safar 1386 AH (June 8, 1966) relating to the Penal Code (Official Gazette, No. 84).

People's Democratic Republic of Algeria. (2009). Law No. 09-04 of 14 Sha'ban 1430 AH containing the specific rules for the prevention of crimes related to information and communication technologies and their combating (Official Gazette, No. 43).

People's Democratic Republic of Algeria. (2015). Law No. 15-04 of 11 Rabi' al-Thani 1436 AH establishing the general rules relating to electronic signature and certification (Official Gazette, No. 6).

Court case:

Microsoft v. United States, No. 14-2985 (2d Cir. 2016).