Cybersecurity and Its Relationship to Information Systems
الأمن السيبيراني وعلاقته بأمن المعلومات



Hamouda Farouk
Blida2 University, hamou01@hotmail.fr,

Received: 20/04/2026 *Accepted: 16/05/2026* *Published:.22/05/2026*

Abstract:

In the present era, cybersecurity has become a crucial element of national security in developed countries, especially with the comprehensive shift towards the digital age in all aspects of life. The core concept of cybersecurity revolves around securing the digital infrastructure of nations, including vital installations and sensitive information systems such as e-government administration systems, military, police, judicial, economic, industrial, commercial, and other systems. Threatening these systems directly endangers national security, prompting countries to establish specialized agencies for cybersecurity protection, thereby making it a top priority for contemporary governments.

Keywords: Cybersecurity; National security; Digital infrastructure; Sensitive systems; Protection agencies.

ملخص:

في العصر الحالي، أصبحت الأمن السيبراني عنصرًا بالغ الأهمية في الأمن القومي للدول المتقدمة، خاصة مع التحوّل الشامل نحو العصر الرقمي في جميع جوانب الحياة. ويتمحور المفهوم الأساسي للأمن السيبراني حول تأمين البنية التحتية الرقمية للدول، بما في ذلك المنشآت الحيوية وأنظمة المعلومات الحساسة مثل أنظمة الإدارة الإلكترونية للحكومات،

والأنظمة العسكرية، والشرطية، والقضائية، والاقتصادية، والصناعية، والتجارية، وغيرها من الأنظمة. ويؤدي تهديد هذه الأنظمة الحساسة إلى تعريض الأمن القومي للخطر بشكل مباشر، مما يدفع الدول إلى إنشاء هيئات متخصصة للحماية السيبرانية، مما يجعل من الأمن السيبراني أولوية قصوى لدى الحكومات المعاصرة.
كلمات مفتاحية: الأمن السيبراني؛ الأمن القومي؛ البنية التحتية الرقمية؛ الأنظمة الحساسة؛ هيئات الحماية.

- Hamouda Farouk [1] hamou01@hotmail.fr,

INTRODUCTION

In an era marked by rapid technological advancement and the pervasive shift toward digitalization in all sectors of life, data has emerged as a strategic and economic asset whose protection is no longer optional but essential. The increasing reliance on interconnected systems, cloud computing, and data-driven operations has led to heightened vulnerability to cyber threats. As a result, the concept of cybersecurity has gained paramount importance, particularly in securing digital infrastructures and maintaining the integrity, confidentiality, and availability of information.

Information security and cybersecurity, while interrelated, serve distinct yet complementary roles. The former emphasizes the protection of data in any form, while the latter focuses on protecting systems, networks, and programs from digital attacks. The integration of both is fundamental in forming a comprehensive approach to information protection, which has become a cornerstone for the sustainable development of digital societies.

To scientifically approach the subject, the problem must be clearly articulated through a guiding question, What is the concept of cybersecurity, and how does it relate to information systems? followed by the formulation of hypotheses: The researcher assumes that cybersecurity is a critical subset of information security, and that understanding its mechanisms, scope, and integration with information systems significantly contributes to building secure and resilient digital environments. It is further hypothesized that the implementation of internationally-aligned cybersecurity frameworks leads to enhanced protection of data and digital infrastructure against cyber threats, and an analytical review of relevant previous studies to identify gaps and justify the need for the present research.

1. The Concept of Information Security and Cybersecurity

Information security and cybersecurity are interconnected concepts aimed at protecting data and information in the digital age, each with a distinct focus and scope.

1.1. Definitions of Information Security and Cybersecurity

The concept of cybersecurity is relatively modern, having emerged in response to the rapid evolution of technology and the digitization of communication and information systems across the globe. Its development is deeply intertwined with the rise of the Internet, the proliferation of digital devices, [1]and the increasing dependence on online services and infrastructure. As cyber threats began to surface—from data breaches and ransomware to state-sponsored cyber espionage—the need for a robust framework to

secure digital environments became urgent. Consequently, the term cybersecurity entered the academic, legal, and policy lexicons as a vital component of national security and organizational integrity.[2]

The word cyber is commonly used to describe anything related to computer networks, the Internet, or digital communication platforms. Cyberspace—a derivative term—denotes the virtual environment formed through the interconnection of digital systems, platforms, applications, and services. This environment hosts a multitude of operations such as online banking, virtual commerce, digital education, e-government, and remote healthcare. In essence, cyberspace encapsulates the infrastructure, systems, and digital footprints that now form the fabric of modern life.[3]

From a linguistic standpoint, the term cyber originates from the Greek word *kybernetes*, meaning "steersman" or "governor," which symbolized control and regulation. American mathematician Norbert Wiener later popularized this root through the term *cybernetics*, describing self-regulating systems and automatic control processes. Over time, cyber has evolved to symbolize digital governance, control, and surveillance across technological systems.

Cybersecurity—or cyber security—broadly refers to the collection of strategies, tools, processes, and policies that ensure the protection of digital environments and assets. These include not only data and software but also the infrastructure and

hardware that support electronic communication. Cybersecurity seeks to ensure:[4]

- Confidentiality: Protecting sensitive data from unauthorized access.
- Integrity: Guaranteeing that data is accurate and unaltered.
- Availability: Ensuring that systems and data remain accessible when needed.

These objectives are achieved through the application of technical, organizational, and administrative measures, ranging from encryption protocols and firewalls to intrusion detection systems and regulatory frameworks. Cybersecurity therefore operates at both micro and macro levels, ensuring protection at the level of individual systems as well as national infrastructures.

Its importance is further amplified by the increasing sophistication of cyber threats, including phishing, malware, zero-day exploits, and advanced persistent threats. As a result, critical infrastructures such as financial systems, energy networks, communication systems, and healthcare services require enhanced protection against disruption.[5]

Scholars and institutions have proposed various definitions of cybersecurity, reflecting its multidimensional nature:[6]

- Martti Lehto & Pekka Neittaanmäki: "A set of measures taken in defense against cyberattacks and their consequences."

- Edward Amoroso: "A collection of tools and methods designed to reduce the risk of attacks on computer systems and networks."
- International Telecommunication Union: "A combination of policies, procedures, technologies, and practices aimed at protecting cyberspace."
- U.S. Department of Defense: "All procedures necessary to ensure the protection of information in all its forms."
- European Cybersecurity Declaration: "The ability of information systems to resist unauthorized access."
- Sami Mohamed Bounif: "A set of mechanisms and policies aimed at protecting electronic communications and data."
- Samir Kelaa Deroussou: "A means of reducing risks associated with cyberattacks on systems and networks."

While cybersecurity and information security overlap, they remain distinct. Information security focuses on protecting data in all its forms, whereas cybersecurity addresses the protection of digital systems, networks, and infrastructures from cyber threats.

1.2. Distinction Between Cybersecurity and Information Security

1.2.1. Information Security

Information security represents a critical and foundational pillar in the broader field of digital and technological protection. It specifically focuses on preserving the confidentiality, integrity, and availability of information and data exchanged across communication networks or accessed through various digital platforms. The core objective of information security is to prevent any unauthorized access, intentional tampering, exploitation, surveillance, or breach of sensitive or classified data—whether by internal actors or external threats[7]. In today's hyperconnected digital age, where individuals, institutions, and governments heavily rely on digital platforms for communication, transactions, data storage, and strategic operations, the need for robust information security systems has never been more imperative.

At its core, information security is designed to create a secure, trustworthy digital environment where data can be processed, transmitted, or stored without fear of exposure, manipulation, or deletion. It is especially concerned with:

- data at rest
- data in transit
- data in use

To achieve this, a multifaceted framework of policies, technical tools, legal standards, and operational procedures must be implemented. These include access control systems, multi-factor authentication, data encryption, firewalls, intrusion detection systems, and security awareness training for users.

Systems for securing programs and applications: Ensuring that all software components are hardened against vulnerabilities and malware.

Systems for securing operating systems: Preventing unauthorized access and system-level exploits.[8]

Systems for securing application entry and exit: Regulating data flow to avoid attacks and leaks.

Systems for securing software and electronics: Integrating hardware-level and firmware protections.[9]

Despite these layers of protection, information security faces continuous challenges such as weak encryption, malware, phishing, and system vulnerabilities. Therefore, it is based on fundamental principles:

1. Confidentiality
2. Integrity
3. Authenticity
4. Non-repudiation
5. Accountability
6. Controlled access

1.2.2. Cybersecurity

Cybersecurity extends beyond traditional information security by protecting entire digital ecosystems, including systems, networks, and infrastructures. It aims to defend against cyber threats such as malware, ransomware, social engineering, and cyber warfare.[10]

Unlike information security, cybersecurity adopts a broader and proactive approach, focusing on detecting, preventing, and responding to attacks across the entire digital environment. It ensures not only data protection but also system resilience and operational continuity.

Cybersecurity mechanisms are designed to monitor and respond to threats in real time, ensuring that systems remain secure and uncompromised.[11]

2. Information Security System and its Relationship to Cybersecurity

The information security system is a comprehensive framework composed of policies, procedures, and technologies designed to protect information assets. It ensures confidentiality, integrity, availability, and authenticity of data.

This system is closely linked to cybersecurity, which functions as a specialized branch focused on protecting digital infrastructures and networks. Thus, cybersecurity can be considered a subset of information security.[12]

2.1. Global Information and Cyber Security Standards

In the digital era, protecting data and infrastructure requires adherence to international standards. These standards guide organizations in implementing effective security measures and ensuring compliance.

Among the most important frameworks are those developed by ISO, IEC, and ITU, as well as COBIT and ITIL, which provide governance and management guidelines.

The International Organization for Standardization (ISO), founded in 1947 in Geneva, is a leading authority in developing global standards, including those related to cybersecurity.

2.1. Global Information and Cyber Security Standards

In an increasingly digitized world, the protection of sensitive data, technological infrastructure, and user privacy has become a global imperative. To achieve a robust, reliable, and adaptive information security system, organizations and governments alike must align their security strategies with internationally recognized standards. These standards constitute comprehensive reference frameworks that guide organizations in adopting best practices, ensuring legal compliance, and fostering interoperability across technological environments.

Global standards act as blueprints for designing, implementing, managing, and auditing information and cybersecurity measures. They also serve as instruments of international cooperation, enabling mutual recognition of secure systems across borders. Among the most widely adopted frameworks are those developed by ISO in collaboration with IEC and ITU, in addition to COBIT and ITIL. [13]

The International Organization for Standardization (ISO), established in 1947 and headquartered in Geneva, remains a

leading authority in the development of global standards, including those related to information security and cybersecurity.

2.1.1. ISO/IEC 27002: Practical Guidance for Information Security Controls

ISO/IEC 27002 provides a set of guidelines and principles for implementing and improving information security management practices within organizations. It supports ISO/IEC 27001 by offering operational controls across multiple domains, including:[14]

- Security policy
- Organizational security structure
- Asset management
- Human resource security
- Physical and environmental protection
- Operations and communications management
- Access control
- System development and maintenance
- Incident management
- Business continuity
- Compliance

2.1.2. ISO/IEC 27001: Information Security Management System (ISMS)

ISO/IEC 27001 establishes a formal framework for managing information security based on the PDCA (Plan-Do-Check-Act) model:[15]

- Plan: Define policies and objectives and conduct risk assessments
- Do: Implement the established controls
- Check: Monitor and evaluate system performance
- Act: Apply corrective and preventive measures

This standard is universally applicable and provides a certifiable structure demonstrating compliance with global security practices.

2.1.3. ISO/IEC 15408: Common Criteria for IT Security Evaluation

ISO/IEC 15408, also known as the Common Criteria, provides a standardized methodology for evaluating the security of IT systems and products. It ensures that both hardware and software comply with international security benchmarks and offers assurance levels that reflect the rigor of evaluation.

2.1.4. ISO/IEC 13335: IT Security Management

ISO/IEC 13335 provides guidance on managing IT security, including conceptual frameworks, practical implementation tools, technical controls, and administrative procedures necessary to maintain system integrity and efficiency.[16]

2.1.5. Benefits of Implementing ISO Standards

The implementation of ISO standards offers multiple advantages, including:

- Regulatory compliance
- Operational efficiency
- Cost reduction

- Risk management
- Increased stakeholder trust
- Competitive advantage
- Development of a security culture
- Business continuity
- Protection of sensitive data

Certification under ISO 27001 reflects an organization's commitment to safeguarding information assets and enhancing institutional credibility.

2.2. Mechanisms for Establishing an Information Security System

In the digital economy, information has become a central strategic asset that drives innovation, efficiency, and decision-making. Organizations rely heavily on data, making its protection a fundamental requirement for maintaining competitiveness and institutional stability.

However, the expansion of digital infrastructures has increased exposure to cyber threats such as phishing, ransomware, insider attacks, and data breaches, which affect both organizational performance and societal stability.

2.2.1. Multidimensional Framework for Information Security

The complexity of modern digital ecosystems requires a multidimensional approach that integrates technical, organizational, and human factors. This framework includes six fundamental domains:[17]

1. Authentication: Ensuring access is granted only to authorized users through secure verification mechanisms.
2. Privacy: Protecting sensitive data through encryption and compliance with legal and ethical standards.
3. Access Control: Regulating access to systems and data based on defined roles and permissions.
4. Integrity: Maintaining the accuracy and consistency of data throughout its lifecycle.
5. Non-repudiation: Ensuring accountability through traceable and verifiable actions.
6. Continuity: Guaranteeing system availability through backup, recovery, and resilience mechanisms.

Implementing an effective information security system requires a structured process that includes risk assessment, deployment of security technologies, development of policies, and continuous monitoring.

Organizations must align their strategies with international frameworks such as ISO 27001, COBIT, and NIST to ensure comprehensive and up-to-date protection.

Ultimately, information security is not merely a defensive mechanism; it is a strategic enabler that strengthens institutional resilience, builds stakeholder trust, and enhances competitive advantage.

CONCLUSION :

This research examined the concept of cybersecurity and its relationship with information systems, concluding that

cybersecurity constitutes a fundamental and strategically critical subset of information security in the digital age. While information security encompasses the protection of data in all its forms—ensuring confidentiality, integrity, and availability—cybersecurity specifically focuses on safeguarding digital systems, networks, and infrastructures against evolving cyber threats such as unauthorized access, data breaches, and cyber espionage.

The study further demonstrated that the implementation of internationally recognized standards, particularly ISO/IEC 27001, 27002, 15408, and 13335, plays a decisive role in strengthening cybersecurity frameworks. These standards provide structured methodologies for risk assessment, control implementation, regulatory compliance, and the development of security-aware organizational cultures.

Moreover, the research highlighted the importance of national cybersecurity strategies, supported by legislative frameworks, institutional mechanisms, and international cooperation, in ensuring the protection of critical infrastructures and reinforcing digital sovereignty.

At the practical level, the study recommended adopting an integrated approach that combines information security policies with cybersecurity technologies, alongside enhancing legal frameworks and promoting awareness and capacity-building initiatives.

However, the research acknowledged several limitations, including reliance on theoretical and secondary sources, the

predominance of Western-based standards, the absence of empirical fieldwork, and the rapidly evolving nature of cyber threats. It also noted the need for broader interdisciplinary approaches that incorporate legal, social, and ethical dimensions in future studies.

Bibliography List :

1. Books

- Boufas (2014), *Cybersecurity and National Security*, Publishing, Country.
- Mahatat (2023), *Cybersecurity in Digital Environments*, Publishing, Country.
- Lehto, Martti & Neittaanmäki, Pekka (2020), *Cyber Security: Critical Infrastructure Protection*, Springer, Switzerland.
- Ben Merzoug (2018), *Information Security Systems*, Publishing, Country.
- Stallings, W. (2017), *Cryptography and Network Security*, Pearson, United States.
- Whitman, M. & Mattord, H. (2021), *Principles of Information Security*, Cengage Learning, United States.
- Ferraiolo, D. et al. (2001), *Role-Based Access Control*, Publishing, Country.
- Samir Kelaa Deroussou (2022), *Cybersecurity*, Publishing, Country.

- Amoroso, Edward (2013), *Cyber Security*, Syngress, United States.
- Hassan Al-Fanni (2023), *Information Security Standards*, Publishing, Country.

3. Journal article

- Porter, M. & Heppelmann, J. (2014), *How Smart, Connected Products Are Transforming Competition*, Harvard Business Review, United States, Vol. 92, No. 11.
- Von Solms, B. & Van Niekerk, J. (2013), *Information Security Governance*, Computers & Security, Elsevier, Vol. 29, No. 4.

5. Internet websites

- European Commission (2016), *General Data Protection Regulation (GDPR)*, detailed web site: https://eur-lex.europa.eu (consulted on 20/04/2026).
- NIST (2012), *Risk Management Framework*, detailed web site: https://www.nist.gov (consulted on 20/04/2026).
- International Telecommunication Union (2011), *Cybersecurity Report*, detailed web site: https://www.itu.int (consulted on 20/04/2026).
- U.S. Department of Defense (n.d.), *Definition of Cybersecurity*, detailed web site: https://www.defense.gov (consulted on 20/04/2026).

[1] Boufas, *Cybersecurity and National Security*, 2014, p. 3, 25.
[2] Mahatat, *Cybersecurity in Digital Environments*, 2023.
[3] Lehto, Martti & Neittaanmäki, Pekka, *Cyber Security: Critical Infrastructure Protection*, 2020.
[4] Ben Merzoug, *Information Security Systems*, 2018, p. 34.
[5] Porter, M. & Heppelmann, J., *How Smart, Connected Products Are Transforming Competition*, 2014.
[6] Von Solms, B. & Van Niekerk, J., *Information Security Governance*, 2013.
[7] Stallings, W., *Cryptography and Network Security*, 2017.
[8] European Commission, *General Data Protection Regulation (GDPR)*, 2016
[9] Cavoukian, A., *Privacy by Design*, 2009
[10] Ferraiolo, D. et al., *Role-Based Access Control*, 2001.
[11] Whitman, M. & Mattord, H., *Principles of Information Security*, 2021
[12] NIST, *Risk Management Framework*, 2012.
[13] Samir Kelaa Deroussou, *Cybersecurity*, 2022, p. 253.
[14] Amoroso, Edward, *Cyber Security*, 2013.
[15] International Telecommunication Union, *Cybersecurity Report*, 2011.
[16] U.S. Department of Defense, *Definition of Cybersecurity*.
[17] Hassan Al-Fanni, *Information Security Standards*, 2023.