journal Of Legal and Economic Studies ISSN 2602-7321/ EISSN 2773- 2649

Vol : 09 No: 01 Year: 2026 Page : 827- 836

Cybersecurity: A Theoretical Reading of the Concept

Dr. Salima Mimouni * [1], University Center of Barika, ALGÉRIE،
salima.Mimouni@cu-barika.dz

PhD student: Rafik Meddour [2], University of Nouakchott, Mauritania,
khayrou.1984@gmail.com

Send Article Date: 24 /01/2026 Date of acceptance of the article: 19/05/2026

Abstract: Technological developments have had a significant impact on the establishment of cybersecurity to counter the growing cyber threats in a rapidly advancing digital environment and a digital society characterised by information accumulation, whether at the level of individuals, groups, or states. This has led to an international trend of studying cybersecurity and mobilising international efforts to encourage security measures to protect personal and collective electronic devices and data. Therefore, the aim of this study was to deconstruct the term cybersecurity and clarify its concept, as well as the theories that explain it, as outlined by researchers and specialists in this field.

Keywords: Cybersecurity, cyber threat, control theory, information theory.

Introduction

Cyber security is one of the most important security issues that requires careful and in-depth study and concerted efforts to provide it, given that technological advances and the proliferation and complexity of networks, systems and tools have exacerbated the problem and made cyber security more difficult, especially with the emergence of increasing cyber threats and risks. Therefore, it is necessary to provide a digital environment that ensures trust in electronic transactions and exchanges within a digital society free from any external threats. This study therefore aims to:

- ✓ Define cybersecurity.
- ✓ Identify the most important dimensions of cybersecurity.
- ✓ Attempt to identify the most important cybersecurity theories.

From this, the following question can be posed: What is the conceptual and theoretical basis of cybersecurity?

To answer this question, the following plan was followed:

Section 1: Cybersecurity: A Conceptual Approach
Requirement 1: Definition of cybersecurity.
Requirement 2: Types of cybersecurity.
Section II: Theoretical framework of cybersecurity.
Requirement 1: Information theory of cybersecurity.
Requirement 2: Control theory of cybersecurity.

Section I: Cybersecurity: A conceptual approach

This section includes a conceptual introduction to cybersecurity through its emergence and addresses its definition and basic dimensions:

Requirement 1: Definition of cybersecurity

This requirement addresses the emergence of cybersecurity, its definition, and its most important military, economic, political, and social dimensions.

First: The emergence of cybersecurity

The concept of cybersecurity is linked to the emergence of cyberattacks, which occurred due to two main factors:

1- The use of computers:

In the mid-1950s, computers were used as a tool for processing and storing information digitally. This was accompanied by the combined efforts of a number of private and public companies, which culminated in the development of the central processing unit (CPU) to facilitate the tasks assigned to it. This developed radically in the following decades until computers became fundamental to the work of many private and public institutions, as well as to everyday life.

2- The emergence of the World Wide Web, or 'the Internet':

The Internet has brought about a dramatic revolution in human life through communication and the rapid transfer of information. Countries rushed to use computers to achieve qualitative leaps in the security and military fields in the early 1990s, to the extent that some people coined the term 'Cyber Cold War' or the arms race.[1]

At that time, what became known as 'phishing attacks' and 'electronic espionage' emerged. With the explosion of the information revolution and the advent of the digital age, a number of researchers considered cyberspace to be the fifth domain of warfare after land, sea, air, and space. There was a need to provide special security guarantees with the emergence of cyber threats and crimes at the beginning of the 21st century. Cybersecurity has become part of the field of security studies, and advanced technologies such as encryption, cloud security, and artificial intelligence threat detection have emerged. However, cyber attacks are a complex

and rapidly evolving field, requiring a security response that keeps pace with their rapid development.[2]

Second: Definition of cybersecurity

The word is derived from the term 'cyber,' meaning the internet, which is derived from the Greek word Kybernetes, which first appeared in science fiction literature and referred to the steering of a ship.

The Oxford English Dictionary defines it as: the study of the effectiveness of human work compared to the effectiveness of calculating machines related to the features and characteristics of computers, information technology, and virtual reality, while the Information Security Glossary defines it as: a cyber attack aimed at controlling websites or electronically protected structures in order to disable, destroy, or damage them.[3]

Richard Kamar has defined it as: defensive measures that detect and thwart attempts by hackers. Edward Amorso defines it as: measures that reduce the risk of attacks on software, computers or networks, including measures and tools used to combat piracy, detect and stop viruses, and provide encrypted communications.[4]

According to international standards and professional literature, cybersecurity is a comprehensive system of policies, procedures, and organizational structures that protect digital assets from hostile acts or accidental disruptions. The ISO/IEC standard defines cybersecurity as: A framework aimed at protecting sensitive data and preventing its compromise during exchange, whether through manipulation, sabotage, or unauthorised access, with a focus on the convergence of information security, network security, and critical infrastructure in cyberspace. This illuminates the decision of the US National Institute of Standards and Technology (NIST), which defines cybersecurity as: the process of protecting information by preventing, detecting, and responding to attacks, with an emphasis on availability, integrity, identity security, confidentiality, and non-repudiation.[5]

Cybersecurity is also defined as: the protection of information systems (hardware, software, associated infrastructure, related data and services) from unauthorised access, damage or misuse, including damage caused intentionally by the system operator or accidentally as a result of failure to follow security and protection procedures.[6]

Cybersecurity is therefore a set of technical and administrative measures that include processes and mechanisms designed to prevent any unintended or unauthorised interference, espionage, or intrusion for the purpose of using or misusing electronic information and data stored on communications and information systems and services, or causing any change or damage to them.[7]

It can be said that cybersecurity aims to: [8]

- ✓ Enhance the protection of operational technology systems at all levels and their components, including hardware, software, services provided, and data contained therein.
- ✓ Respond to information security attacks and incidents targeting government agencies and public and private sector institutions.
- ✓ Providing a secure and reliable environment for transactions in the information society.
- ✓ Ensuring the resilience of critical infrastructure to cyber attacks.
- ✓ Providing the necessary requirements to reduce the risks of cybercrime targeting users.
- ✓ Eliminating vulnerabilities in computer systems and mobile devices of all types.
- ✓ Closing gaps in information systems.

Second requirement: Types of cybersecurity

Cybersecurity encompasses several types, including network security, application security, data security, cloud security, endpoint security, and infrastructure security, as follows:

First: Network security

Network cybersecurity is an important area of information technology infrastructure. Therefore, network security assessment and testing should take into account the features and security of network equipment identified as security gateways. Test information is a type of structure according to which network links and nodes are connected, in terms of the number and type of physical or logical security gateways, where cybersecurity relates to external risks, and network security guards against unwanted interference with malicious intent on internal networks.[9]

Network protection ensures stable training networks by preventing unauthorized access to infrastructure. Security departments use machine learning (ML) to detect suspicious traffic and alert to threats in real time for network security monitoring. Network protection refers to all mechanisms that maintain network security against unwanted access and unauthorised interference. A reliable network architecture protects the integrity of the internal network. Protection uses multiple

means, including hardware and software designed to protect data and the network by monitoring connections and preventing attacks from spreading across networks. It uses various tactics to deter malware or other data breaches.[10]

Second: Application security:

This refers to improving application security by raising protection levels through secure software to prevent errors that may increase security risks and protect applications from hacking attempts.[11]

Third: Data security:

This is achieved by storing system data on an external device that is not connected to the computer system and encrypting it with a unique encryption key during transfer and storage. Encryption technologies can also be used to secure data during network transfers and protect it from espionage and unauthorised use. In addition, data loss prevention technologies can be implemented to prevent unauthorised data leaks by backing up data for recovery in the event of loss.[12]

Fourth: Cloud security:

Some believe that information is only secure when managed on an internal network, while others believe that cloud computing can provide the necessary security to preserve and maintain the integrity of information. Cloud computing enables the storage of increasing amounts of data, including personal data, in an online cloud. When stored, personal data is transferred over the internet, which may pose a real threat to an individual's ability to control that personal data. [13]

Third requirement: Dimensions of cybersecurity

Cybersecurity includes military, economic, social, political and humanitarian security systems that aim to maintain stability and security from all cyber threats. Integrated security includes aspects that contribute to strengthening the cybersecurity system, the most important dimensions of which are as follows:

First: The military dimension:

This dimension aims to maintain the ability of military units to communicate via military networks, which facilitates the exchange of information. The idea of creating and deploying an internet network and remote targets is being proposed, but this is a weakness, especially if it is not secure. The destruction or blackmail of military databases could disrupt communications between command units and military units, in addition to the risk of losing control of certain weapons, such as drones, guided missiles, and satellites.

Second: The economic dimension:

Given the use of computers in the operation and development of industries and the driving force behind the economy, the internet is the basis for trade, finance, and financial transactions, all of which are interconnected through computer networks to ensure cybersecurity, which is particularly relevant to the financial sector.[14]

Third: The social dimension:

There are more than 4 billion internet users worldwide, with more than 2.4 billion people using social networking sites. Social networking sites have the highest rates of human interaction, providing ample opportunities to share ideas and successful experiences, but in return they expose personal information to illegal use by external parties, threatening social peace in countries due to the loss of social cybersecurity. [15]

Fourth: The political dimension:

Apart from the leaks of confidential documents and privileges that often lead to diplomatic crises between countries, Russia's cyber interference in the US elections is the most important evidence of the need for cybersecurity and its importance in the political dimension.

Section II: The theoretical framework of cybersecurity

Cybersecurity, like many concepts, contains a set of theories that seek to deconstruct terminology. The most important cybersecurity theories are as follows:.

First requirement: Encryption theory:

This section addresses the general framework of the encryption theory that achieves cybersecurity and the most important advantages and objectives of encryption in providing protection for information, as follows:

First: Definition of encryption theory:

This refers to secret writing with the aim of concealing the true meaning of the message. This approach aims to keep information secure and confidential as it passes through using codes[16] .

Encryption involves providing a specific key or secret shared between the parties involved in the encryption process, in addition to agreeing on a common encryption algorithm in cases where the sender and receiver do not share the same physical carrier. The data must be decrypted and re-encrypted at each point of passage as it travels to the recipient. Encryption is typically used at the link level in the absence of encryption at higher levels[17]

Link-level encryption is also a mechanism for securing data as it travels between two points connected to the same physical link. They can also be connected via two physical links connected to a signal repeater, as is the case with satellite links. Link-level encryption protects protocols or data passing through the physical link from prying eyes.[18]

Second: Advantages and applications of encryption:

Data encryption provides increasingly secure communications, and its most important benefits include the following:

- **Data confidentiality:** Encryption protects personal and financial data and information, and its use is increasing in banking transactions, email, and data exchange between government agencies and companies.[19]
- **Authentication:** It is used to verify the identity of senders and recipients in the message exchange process and ensures that there is no impersonation or manipulation of content during transmission.
- **Integrity**: It ensures data integrity by using verification techniques and detecting any changes.
- **Non-repudiation**: Encryption technologies provide non-repudiation, ensuring that individuals cannot deny sending or receiving information after it has been executed, which is important in legal and commercial transactions where verification of data integrity and the parties involved is essential. [20]

Requirement 2: Control theory

This requirement addresses the definition of control theory, which is considered the basis of cybersecurity, and the types of security that this theory encompasses.

The concept of control in cyber theory is the organisation of the system and deals with the behaviour of dynamic systems and shadows through determinants to maintain the system's plan and path and preserve its outcome, or to plan or to address discrepancies and anomalies in system inputs. It relies on sensors, comparisons, and action generators to manage andcontrol the behaviour of devices and systems associated with the system. The types of control vary as follows[21] :

- ✓ Logic Control
- ✓ Control On-Off
- ✓ Proportional Control
- ✓ Linear control[22]

Conclusion:

Based on the above, it can be said that the concept of cybersecurity has been and continues to be a subject of interest and research for many academic researchers and specialists in the field of security, given the extreme importance and sensitivity of this concept, especially since it poses a direct threat to individuals and, beyond that, to the security of states and organisations.

Findings of the study:

- ✓ The concept of cybersecurity is one of the security concepts that requires a great deal of ongoing research to achieve and succeed.
- ✓ Cybersecurity refers to a set of rules, data and procedures that contain a set of codes that guarantee the privacy of individuals and states.

- ✓ In order to ensure the security and safety of states and individuals, there must be a digital framework that provides extremely accurate and continuous security protection.

Proposed recommendations.

- ✓ A comprehensive and precise security system must be established to deal with the ongoing cyber threat.
- ✓ Individual and international efforts must be combined to enable the early detection of cyber piracy, which has become an invasion of many sensitive sites.

The concept of cyber security should be enshrined at the academic and scientific levels.

* Salima.Mimouni.

[1]- Fares Muhammad Al-Ammarat, Cybersecurity: Concept and Challenges of the Age, Dar Al-Khaleej, Jordan, 2022, p. 24.

[2]- Ali Ibn Ahmed Ibn Taraz, Cybersecurity: The Necessity of Awareness and the Imperative of Implementation, Academic Book Centre, 2025, pp. 33, 34.

[3]- Adris Attia, The Place of Cybersecurity in the Algerian National Security System, Masdaqia Magazine, Issue 1, 2019, pp. 104, 105.

[4] - Ibid., p. 104.

[5]- Abdullah Musa Muhammad Al-Sahlout, Digital Transformation: Between the Possibilities of Artificial Intelligence and the Challenges of Cybersecurity, Dar Al-Yazouri, Jordan, 2025, p. 121.

[6]- Farah Yahya Za'atara, Cyber Threats to US National Security, Al-Arabi Publishing and Distribution, 2023, p. 22

[7]- Abdul Rahman Ali Al-Laqani, The Role of Cybersecurity in Enhancing Electronic Financial Information Security, Dar Al-Yazouri, Jordan, 2022, p. 151.

[8] - Ibid., p. 152.

[9]- Firas Aqil Al-Duwairi, Big Data and Its Role in Reducing Cybercrime under the Cybersecurity Strategy, Dar Al-Khaleej, 2023, p. 79.

[10]- Ibid.

[11]- Cybersecurity: Its Concept and History, 19/9/2024, obtained from: http://www.aljazeera.net Date of access: 08/05/2025.

[12]- Same reference.

[13]- Karima Ahmed, Asma Al-Sayed Mohamed Abdel-Samad, Artificial Intelligence Applications and the Future of Education Technology, Dar Al-Manhal, 2020, p. 153.

[14] - Hassan Nayef Mubarak Al-Hajraf, The Role of Artificial Intelligence in Enhancing Cybersecurity: A Theoretical Perspective, Journal of Comprehensive Research Studies, Issue 5, 2024, pp. 1482, 1483.

[15] - Hassan Nayef Mubarak, op. cit.

[16] -Encryption in Cybersecurity, obtained from: http://mo3lalemllhase.com Date of access: 05/0/2025.

[17]- Ayman Ahmed Ali Al-Hadi, Cybersecurity in the Age of the Knowledge Explosion, Dar Al-Yawori, Jordan, 2022, pp. 15, 16.

[18]- Ibid.

[19]- Encryption in Cybersecurity, previous reference.

[20]- Ibid.

[21] Salwa Abu Al-Ala Mahmoud, Walid Al-Ghamri Barakat, Creative Thinking in Cybersecurity Theory (Control and the Future) as an Introduction to Enriching the Media Arts , Journal of Architecture, Arts and Humanities, Volume 8, Issue 39, May 2023, p. 417.

List of references:

First: Books:

1. Ahmed Ali Al-Hadi, Cybersecurity in the Shadow of the Knowledge Explosion, Dar Al-Yawri, Jordan.
2. Abdullah Musa Muhammad Al-Sahlout, Digital Transformation: Between the Possibilities of Artificial Intelligence and the Challenges of Cybersecurity, Dar Al-Yazouri, Jordan, 2025.
3. Ali Ibn Ahmad Ibn Taraz, Cybersecurity: The Necessity of Awareness and the Imperative of Implementation, Academic Book Centre, 2025.
4. Farah Yahya Za'atara, Cyber Threats to US National Security, Al-Arabi Publishing and Distribution, 2023.
5. Karima Ahmed, Asma Al-Sayed Mohamed Abdel-Samad, Artificial Intelligence Applications and the Future of Education Technology, Dar Al-Manhal, 2020.
6. Firas Aqil Al-Duwairi, Big Data and Its Role in Reducing Cybercrime under the Cybersecurity Strategy, Dar Al-Khaleej, 2023.
7. Abdul Rahman Ali Al-Laqani, The Role of Cybersecurity in Enhancing Electronic Financial Information Security, Dar Al-Yazouri, Jordan, 2022, p. 151.

Second: Articles:

1. Salwa Abu Al-Ala Mahmoud, Walid Al-Ghamri Barakat, Creative Thinking in Cybersecurity Theory (Control and the Future) as an Introduction to Enriching New Media Arts, Journal of Architecture, Arts and Humanities, Volume 8, Issue 39, May 2023, p. 417
2. Hassan Nayef Mubarak Al-Hajraf, The Role of Artificial Intelligence in Enhancing Cybersecurity: A Theoretical Perspective, Journal of Comprehensive Research Studies, Issue 5, 2024, pp. 1482, 1483.

3. Adris Attia, The Place of Cybersecurity in the Algerian National Security System, Masdaqia Journal, Issue 1, 2019, pp. 104, 104.

Third: Websites:

1. Cybersecurity: Its Concept and History, 19/9/2024, obtained from: http://www.aljazeera.net Date of access: 08/05/2025.

2. Encryption in Cybersecurity, obtained from: http://mo3lalemllhase.com Date of access: 5 May 2025.