

The Autonomy of Electronic Technology and Its Role in Strengthening Cybersecurity in African Countries

Elhamza Ahmed

Echahid Cheikh Larbi Tebessi University, ahmed.elhamza@univ-tebessa.dz

Received: 09/04/2025

Accepted: 11/06/2025

Published: 19/06/2025

Abstract:

This study emphasizes the significance of electronic independence for African countries, which have heavily relied on imported digital technologies, increasing their vulnerability to cyber threats such as advanced attacks, fraud, data theft, and espionage. To combat these risks, it is crucial for these nations to enhance awareness of cybersecurity issues and educate users on best practices. Implementing training programs can help employees and users understand electronic risks and how to mitigate them effectively. Additionally, investing in local electronic infrastructure and developing technical capabilities is essential. Promoting collaboration between the private and public sectors in technology production and development will further support the necessary independence to address various cyber threats effectively.

Keywords: Electronic independence; infrastructure; cybersecurity; African countries.

Corresponding author: Elhamza Ahmed, *e-mail:*. ahmed.elhamza@univ-tebessa.dz

INTRODUCTION:

The importance of cyberspace as a national security issue has increased due to the growing international reliance on it for managing the cosmic infrastructure of information. On the other hand, the escalating frequency of attacks by hackers, who may be backed by hostile entities, states, or even terrorist groups, poses increasing risks to both civilian and military facilities. This raises the issue of cyberspace security as an international concern, given its significance across economic, political, security, and social dimensions.

The relationship between cyberspace and various vital entities, whether civilian or military, highlights the possibility of them being targeted through cyberspace. Such attacks can either target cyberspace as a medium and carrier of services or cripple their information systems, thereby impacting their functionality. Consequently, controlling and executing such attacks becomes a strategically crucial tool of control and influence, both in times of peace and war.

Given these circumstances, it is evident that the issues of cyber independence and cyberspace security have become international priorities, garnering increased attention in many countries' national security agendas. Addressing these issues necessitates the development of a specific strategy that primarily recognizes the relationship between cyberspace security, national security, and the issues of economic and social development and political stability. Moreover, it emphasizes the importance of understanding the legal aspects related to communication technology and information, their misuse, and the need for the existence of an organizational or institutional structure to confront these risks during emergencies.

By clarifying the relationship between the capabilities and technical capacities of communication and information technology, their potential misuse, and understanding associated risks and response mechanisms, the role of human resources in achieving cyber independence becomes apparent. This role entails implementing security measures to secure technology resources and the need for collaboration among all stakeholders in the

global information community to establish a global culture of cyberspace security.

In the present time, the digital revolution and the world of the internet have become environments that regulate numerous economic, administrative, and research activities. They also serve as platforms for interaction, communication, and innovation, where it is no longer possible to do without internet networks, communication tools, and data storage and information technologies. This is evident in the trend towards electronic governance, electronic economy, and the management of various types of information and data, which are often transmitted and stored through computer networks. Hence, the importance of securing these networks against various threats and risks has become necessary. This gave rise to what is known as "cyber independence" or electronic information security, which has become an integral part of any national security policy. Developing countries, in particular, view it as a counterpart to traditional security, expressing their sovereignty and national security. Consequently, decision-makers in most countries classify electronic information security issues as a priority in their national defense policies.

Cyber independence means protecting the set of technological and administrative means used to prevent unauthorized use of computer networks, exploiting vulnerabilities, and recovering electronic information contained within them. Its aim is to ensure the continued operation of information systems, secure the protection, confidentiality, and privacy of data, whether belonging to individuals, organizations, or states in cyberspace. This is achieved by seeking to secure and protect data privacy concerning individuals, institutions, or countries.

How can cyber independence enhance cybersecurity, particularly in developing countries?

This primary question encompasses the following sub-questions:

- What is the concept of cyber independence?
- What is the concept of cybersecurity?
- What are the major cyber threats?
- How can cyber independence be achieved?

- What are the key mechanisms to enhance cybersecurity in developing countries?

To answer these questions, the following main hypothesis can be formulated:

The achievement of cyber independence leads to the enhancement of cybersecurity, especially in developing countries.

Section I: The concept of electronic technological independence:

The discussion of electronic technological independence for devices and means cannot be addressed unless they are independent of the controlled unit and secure from external influence. Although these devices cannot be completely independent due to technological dependency, the need to work on solutions to reduce reliance on imported technology has become an urgent necessity to partially alleviate the electronic dependency on advanced countries. This concept will be implemented as follows:

A) Definition of Electronic Technology:

Electronic technology can be defined in several ways, including the following: (Ouissi & Ghareebi, 2022, p. 13)

- Electronic technology is defined as: "those electronic devices consisting of hardware and software that process data after encoding or encrypting it into binary signals. These devices are often computers."

- It is also defined as: "obtaining audio, visual, and digital information in written form, processing, storing, and transmitting it using a range of micro-electronic computing and remote communication equipment."

- Some see it as: "not only the transfer, processing, storage, and management of information for a wide range of individuals and institutions but also the continuous differentiation between those who generate information (innovation) and possess the ability to exploit it (skills) and those who consume it with limited skills." (Omahi & Bouadi, 2019, p. 195)

B) Definition of Electronic Technological Independence

The state of technological dependence refers to the condition in which technology is primarily approached as a recipient and consumer rather than an active participant. In the best-case scenario, it is viewed as an imitator, far removed from the innovative technology-generating groups.

However, the issue here is relative, as even the most technologically advanced societies import and consume products from other communities and engage in defined trade and knowledge exchange relationships. Civilization and knowledge, in general, grow dynamically through communication and exchange with others.

The problem arises when this exchange relationship, in terms of material and knowledge, becomes unidirectional rather than reciprocal. In development and technological transformation studies, this is referred to as technological colonization. Today, most developing countries implicitly or explicitly seek to overcome this situation by striving for technological independence. (Ramadan, 2019)

Therefore, technological independence means the ability to engage with the rest of the world in mutually beneficial exchange relationships concerning technological products and services, with a level of equality and decision-making independence. It also means possessing the necessary local competence in the technological field to internally address the basic needs of its members, including human development needs. In short, technological independence can be defined as the stage at which a community possesses the capability to determine its destiny in technological matters. Any sustainable development project in a developing country should be measured by the extent to which it achieves this independence.

Thus, electronic independence is a multidimensional process that requires a focus on infrastructure, software, security, policies, and local cooperation. By achieving electronic independence, countries and institutions can attain sovereignty and control over digital technology and data, thereby enhancing security and sustainable development in the digital age. (Erber, p. 422)

C) Translation: The Importance of Electronic Technological Independence

Electronic technological independence refers to the ability to develop and utilize electronic and information technology independently, with

minimal dependence on external entities. Its importance lies in the following aspects: (Gumahad, April 1996, pp. 156-157)

1. Achieving Technological Sovereignty: Through electronic technological independence, countries and institutions can control and develop the technology they use according to their unique needs. This allows them to rely on local technological resources and enhance their own technological capabilities, contributing to achieving independence and technological sovereignty.

2. Security and Privacy: With electronic technological independence, relevant entities can implement security and protection measures that meet their specific requirements. It enables the improvement of data security and protection of sensitive information by providing specialized technological solutions and independent management.

3. Integration and Compatibility: Electronic technological independence enables relevant entities to better coordinate and integrate their information and communication technology with internal processes and systems. This enhances work efficiency and simplifies integration between applications and digital infrastructure.

4. Development and Innovation: With electronic technological independence, organizations and countries can innovate and develop technological solutions that meet their unique needs and enhance their competitiveness. Independent technology can be adapted to the institution's requirements and its ability to adapt to future changes.

D) Mechanisms for Achieving Electronic Technological Independence

In light of the current geopolitical changes and fluctuations, the issue of technological independence for countries becomes of utmost importance. With the increasing international interventions that impose restrictions on investments and technology exports, technological security and innovation have become subject to external decisions. Therefore, every country must prioritize the development of its national workforce and equip them with skills that align with contemporary technological challenges.

This requires enhancing educational and training programs to include advanced disciplines such as programming, cybersecurity, big data analysis,

and cloud computing. Additionally, it is important to invest in research and development and provide support for national startups to encourage innovation and independence. Furthermore, it is necessary to encourage young people to explore and innovate in technological fields and provide them with opportunities to implement their projects and ideas. Governments should be active partners in this process by providing the necessary infrastructure and supportive policies that facilitate creativity and development.

The path to achieving technological independence may be long and filled with challenges, but it is not impossible. By directing investments towards building national capabilities, enhancing technological infrastructure, and developing young talents, a technological future built on national expertise and talents can be envisioned. These efforts will serve as the foundation for countries to secure a position at the forefront of global innovation and compete strongly in the global market.

Therefore, electronic technological independence has become not just an option but a strategic necessity. It requires continuous and coordinated efforts to build a new generation capable of leading the technological renaissance and enhancing national security and economic independence. Technology is not only a means of progress but also a symbol of national sovereignty and dignity. (Al-Abassi)

Section II: The Concept of Cybersecurity

The concept of cybersecurity refers to the protection of electronic systems, networks, and data from threats in the cyberspace, while ensuring their integrity and confidentiality. It entails safeguarding digital systems and sensitive information against unauthorized access, manipulation, damage, and tampering. The concept of cybersecurity encompasses a wide range of challenges and threats, including cyber-attacks, malware, electronic espionage, online fraud, digital identity theft, cyber piracy, and others, which will be further elaborated as follows:

A) Definition of Cybersecurity

To understand cybersecurity, we can consider prominent definitions as follows:

Richard A. Kemmerer defines cybersecurity as "a defensive means aimed at detecting and thwarting attempts made by hackers." (Mokhtar, 2015, p. 05)

Edward Amoroso defines cybersecurity as "means aimed at reducing the risk of attacks on software, computer devices, or networks. It includes tools used to counter hacking, detect and stop viruses, and provide encrypted communications." (Mokhtar, 2015, p. 05)

It is worth noting that both Richard Comer and Edward Amoroso focused in these definitions on considering cybersecurity as a defensive measure against attacks and hacking operations targeting various computers and networks.

According to the definition provided by the International Telecommunication Union (ITU), cybersecurity is described as: "The collection of tools, policies, security concepts, security safeguards, risk management approaches, actions, training, best practices, assurance mechanisms, and technologies that can be used to protect the cyber environment and organization assets and users." (Mokhtar, 2015, p. 05)

The cyber environment includes computer devices, software, applications installed on them, interconnected networks, human elements, infrastructure, and communication systems. It also encompasses all information, whether stored on devices or transmitted between them. Cybersecurity aims to preserve and protect this environment from cyber risks and threats.

This definition illustrates that cybersecurity encompasses all policies, measures, tools, and approaches to risk management and the protection of the cyber environment against cyber risks and threats. It involves safeguarding information through three main dimensions: personal information, internal corporate information, and cross-border information.

According to the Oxford dictionary, cybersecurity is defined as "the measures and precautions taken to protect electronic information from unauthorized or criminal use." (Mokhtar, 2015, p. 05)

Cybersecurity can also be defined as the "reduction of the risk of harmful attacks on software and computer devices, including tools used to

detect intrusions, stop viruses, and prevent unauthorized access." (Craigén&Others, Octobre 2014, p. 14)

Based on its objectives, cybersecurity can be defined as the "activity that ensures the protection of human and financial resources associated with information and communication technologies, and guarantees the ability to mitigate losses and damages resulting from risks and threats. It enables the restoration of the situation to its original state as quickly as possible, so that production processes do not halt and damages do not turn into permanent losses." (Jubour, 2012, p. 03)

It is evident from this definition that protecting human and financial resources and everything related to information and communication technologies is one of the goals of cybersecurity. The purpose is to minimize losses and damages and prevent them from becoming permanent, thereby ensuring the continuity of production processes.

In conclusion, discussing cybersecurity leads to the following points:

- Cybersecurity encompasses the defensive means, tools, and policies to confront various cyber threats and hacking operations in order to protect the cyber environment.

- Cybersecurity ensures the capability to mitigate losses and damages and contain them as quickly as possible, preventing them from turning into permanent losses.

- Cybersecurity is a strategic weapon in the hands of governments and individuals, especially since cyber warfare has become an integral part of modern tactics in conflicts and attacks between nations.

B) Dimensions of Cybersecurity

Cybersecurity is associated with various fields, including political, military, economic, legal, and social domains, with the aim of achieving an integrated security system that works to preserve the national security of a state from any potential cyber threats. This can be further explained as follows:

1- Military Dimension

The relative advantage of cyber power lies in its ability to interconnect military units through military networks in cyberspace,

allowing for easy exchange and flow of information, rapid issuance of military orders, and the capability to remotely target and destroy objectives. However, this advantage can turn into a vulnerability if the electronic network used for these purposes is not well-secured against external breaches, which could result in launching counter-cyber attacks on military force networks and intelligence systems. This could lead to the destruction of military databases, the disruption of the state's ability to rapidly deploy its capabilities and forces, the severing of communication systems between military units, and the disabling of computer networks.

Furthermore, it is possible to paralyze air defense systems, electronic guidance systems of the adversary, as well as the potential loss of control over command and control units, in addition to the enemy's loss of ability to control or communicate with satellites. (Mokhtar, 2015, p. 06)

2- Economic Dimension

Cybersecurity is closely tied to the economy, as there is a clear correlation between the knowledge economy and the expanded use of information and communication technologies. It is also closely linked to the value represented by data and the information that is exchanged, stored, and utilized at all levels. Information and communication technologies enable the enhancement of economic development for many countries by benefiting from the utilization opportunities provided by international and major companies, which seek to manage their production costs under optimal conditions. (Jubour, 2012, p. 30)

Additionally, the world has entered the era of electronic finance within a dynamic technological environment after the launch of electronic services. Investments in digital finance by banks and financial institutions are increasing, and companies are competing to develop applications that facilitate secure payment mechanisms. Some countries have enacted specific legislation to protect their funds and address the potential difficulties and challenges arising from this, including legislation aimed at curbing serious economic and financial crimes that transcend borders, such as money laundering and tax evasion.

Therefore, cybersecurity ensures the provision of services delivered through information and communication technologies, as well as their widespread adoption, which translates practically into the development of a robust economic foundation. (Jubour, 2012, p. 31)

3- Political Dimension

The political dimension of cybersecurity primarily involves the right of a nation to protect its political system, entity, and economic interests, which signify its duty and obligation to strive for the welfare of its people while internal power dynamics are at play. Individuals have now become significant players in the political game, as they have the ability to access vast amounts of information that provide insights and justifications for the political decisions made by their government. (Jubour, 2012, p. 29)

Conversely, those involved in the political sphere do not hesitate to leverage these technologies to reach the widest possible audience and promote their policies on a global scale. The impact of this is significant, regardless of the validity of the policies, principles, and positions being promoted. For example, during his election campaign, Obama extensively utilized social networks, and the leaked thousands of classified diplomatic documents through WikiLeaks had a negative impact on diplomatic relations between nations. (Jubour, 2012, p. 30)

4- The Social Dimension

Social media platforms, in particular, contribute to opening up opportunities for individuals to express their political aspirations and social ambitions in various forms. They also serve as a means for the participation of all segments of society and its components in community development, providing an opportunity to access ideas and information that are needed by society to maintain the stability of the digital space and the society that relies on it. Additionally, the openness of a community to other societies establishes the exchange of experiences, ideas, and the formation of prospects for cooperation and integration.

Furthermore, this digital space offers capabilities and capacities for scientific, cultural, and service fields, allowing access to remote areas and specific demographics. It also plays a role in information exchange during

times of crisis and disasters, ensuring that assistance is provided promptly. (Jubour, 2012, p. 31)

Moreover, it contributes to preserving the core values of society, such as belonging, beliefs, customs, and traditions, through the establishment of groups that focus on raising awareness about these issues. In this context, international organizations and entities emphasize the importance of promoting a culture of security in the digital space and the need for cooperation among all segments of society to achieve and ensure its protection from cyber threats that negatively impact societal ethics and recruit individuals for issues that affect international security and peace.

Therefore, it is necessary to build a responsible and aware society about the risks of the digital space, capable of dealing with a minimum level of safety rules while recognizing the legal consequences that may arise from certain actions practiced in the digital space. (Mokhtar, 2015, p. 07)

5- The Legal Dimension

The relationship between law and technologies is a reciprocal one. The different technological advancements necessitate corresponding legal regulations to keep pace with them. This involves establishing frameworks and legislation for both legal and illegal activities. However, generally speaking, cybercrime currently lacks strict legal frameworks to effectively address it. This may be attributed to factors such as the inherent nature of electronic crime itself, the difficulty in identifying perpetrators of such crimes, and the flexibility of definitions associated with information technology. Additionally, cybercrimes are not confined by national borders, which requires activating international cooperation to combat them. (Mokhtar, 2015, p. 07)

C) Sources of Cyber Threats

The main sources of cyber threats can be described as follows:

1- Botnet Operators: These are networks controlled by remote command and control systems to coordinate attacks and distribute phishing schemes, spam messages, and malicious attacks.

2- Competing Companies: These are companies that target other organizations with the aim of obtaining sensitive information to improve their competitive advantage in various fields.

3- Criminal Groups: Criminal groups seek to attack systems for financial gain. They specifically utilize spam messages, phishing, spyware, malware, and online fraud. (Op-cit)

4- Nation-States: Intelligence agencies utilize cyber capabilities for information gathering and espionage. Many countries heavily invest in developing information warfare doctrines, programs, and capabilities. These capabilities enable countries to have a significant and dangerous impact by disrupting supplies, communications, critical infrastructure, and the economic structures that support military power.

5- Network Intrusion Hackers: These groups aim for revenge, targeting others, monetary gain, and obtaining unauthorized information. This requires a high level of skill and computer knowledge. Hackers can download attack scripts and protocols from the internet and launch them against victim websites. Attack tools have become more advanced and easier to use. (Op-cit)

6- Spyware/Malware: Individuals or organizations execute attacks against users by producing and distributing spyware, malware, and various destructive computer viruses, including the Melissa virus, the Nimda worm, the Code Red worm, the Slammer worm, and the Blaster worm.

7- Terrorist Groups: These groups aim to destroy, disable, or exploit vital infrastructures to threaten national security, cause mass casualties, and weaken economies of nations. However, despite this, the U.S. intelligence agency views these groups as a limited cyber threat and expects them to primarily focus on traditional attack methods.

D) Types of Cyber Threats

The vulnerabilities and points of exposure in digital technology combine to create an environment of insecurity. The evolution of the Internet has been accompanied by the evolution of cybercrime in its various forms and methods. New technologies have the potential to facilitate all types of cyber threats, which can be referred to and highlighted as follows:

1- Electronic Crime

Electronic crime, also known as cybercrime, has evolved over time with the development of information technology. It has been referred to by various names, starting with "misuse of computers" and "computer fraud," then progressing to "cybercrime," "computer-related crimes," "high-tech crimes," "internet crimes," and finally "cybercrime."

Electronic crime is defined as "a set of illegal actions and activities carried out through electronic equipment, devices, internet networks, or content transmitted through them. It is a type of crime that requires knowledge of computer technology and information systems to commit, investigate, and prosecute." (Bonara, p. 03)

Many scholars have adopted the definition of cybercrime given by the Organization for Economic Cooperation and Development (OECD) in a meeting held in Paris in 1983, which defines it as "any illegal, unethical, or unauthorized behavior related to the processing or transmission of data."

Electronic crime can be defined as: "All forms of intentional and unlawful behavior committed using computer systems connected to the internet, which compromise the system, its contents, or the operations conducted through it, with the purpose of causing harm to the victim, financial gain, or other objectives, by individuals who possess full knowledge of information technology techniques and secrets."

2- Malicious Software

Malware, which stands for Malicious Software, refers to software designed with malicious intent. Malicious software aims to harm, disable, gather information, spy, or disrupt computer operations. It can illegitimately infect a computer system without the user's knowledge or consent in order to compromise the device and spy on it. (Tawilah, p. 10)

Some types of malware include:

2-1-Trojan Horses :

Trojan horses are programs that contain hidden instructions aimed at sabotage and causing harm to the system, despite appearing to perform normal functions. They deceive the user into believing that they are carrying out a specific task while, in reality, they perform a different

destructive action. They can sometimes spy on and monitor all activities and record data on the infected device. At other times, they may cause various types of damage to infected devices, such as encrypting or deleting data. Trojan horses cannot replicate themselves or attach to other programs, but they carry out a specific task designed for them. (Bumflah, p. 15)

2-2- Logic bombs and time bombs :

are types of Trojan horses. Logic bombs are triggered by a specific logical condition, such as reaching a certain number of employees or removing a specific employee's name from the payroll list. They can also be triggered by typing a specific word or running a particular program a certain number of times. On the other hand, time bombs are activated based on a specific timing, such as a specific hour or a specific day. (Bumflah, p. 15)

2-3-Worms:

Worms do not require another program to attach to in order to carry out their functions, unlike viruses that require a host to execute their tasks. Worms operate independently, having the ability to self-replicate and move from one file to another and from one device to another connected to the network to achieve their spread.

Worms do not typically aim to sabotage or destroy files like viruses do. However, they can cause an increased burden on network traffic by consuming memory, processor, disk, and other computer resources, potentially leading to system crashes or slowdowns. (Bumflah, p. 06)

3-Hacking

Referred to in the English language as "Hacking," it is called "Tajassus" or "Al-Qurssana" in Arabic. It involves unauthorized individuals gaining illicit access to a computer's operating system for purposes such as espionage, theft, or sabotage. The infiltrator, known as a hacker, can move, delete, or add files and programs. They can also take control of the operating system, issuing commands such as printing, capturing images, or storage operations (Jabir). As a result, the targeted individual, whether an individual, organization, or nation, becomes vulnerable to information theft,

data breaches, infrastructure damage, or security threats. (Al-Awadi, August 2016, p. 19)

Hackers possess high-level programming skills and a deep understanding of computer operation, which facilitates their ability to breach and modify systems. There are two types of hackers:

3-1- White Hat hackers:

White Hat hackers are typically highly intelligent individuals who have complete control over computers and can make programs do things far beyond their original capabilities. This is why we find that some global companies employ hackers like these to benefit from their abilities, whether in technical support or even in finding security vulnerabilities in the systems of these companies. (HASSAN, p. 12)

3-2- Black Hat:

They are individuals who unlawfully harness their intelligence and focus on studying computers and programming in order to steal others' personal information. These malicious actors sometimes alter financial information of companies, sabotage security systems, and engage in other destructive activities. (HASSAN, p. 12) In the worst cases, they completely annihilate the electronic information system. Many of them steal and distribute software for free, often inserting malicious patches among the files of these programs. (HASSAN, p. 13)

Regarding the types of hacking, they can be divided into three categories as follows:

- Server and mainframe hacking involves breaching the servers and main systems of companies, institutions, or government entities by bypassing the firewall through a process called simulation. Simulation refers to impersonating someone to gain access to the system. The IP address contains the sender and recipient addresses, and these addresses serve as crucial information and a significant vulnerability for professionals.

- Personal device hacking involves infiltrating personal devices and covertly extracting the information they contain. This method is very common among both amateurs and professionals.

-Exposing data during transmission and decrypting it if it is encrypted. This method is common among professionals who attempt to steal bank credit card numbers and uncover their secret codes. (Al-Awadi, August 2016, p. 20)

Cyber attacks conducted over the internet or cyberspace are characterized by their ease, as these attacks are carried out remotely. The hacking process requires two essential elements: the first is the controlling software, which resides on the attacker's device, and the second is called the server, which exists on the victim's device and facilitates the hacking process.

It is worth mentioning that hacking methods vary, multiply, and evolve with the advancement of technologies. However, the fundamental element remains the necessity of a connection between the hacker's device and the victim's device. (Al-Awadi, August 2016, p. 20)

4- Viruses

Viruses are considered one of the most dangerous threats to cybersecurity. The presence of a virus indicates a cybercrime, as viruses aim to take control of a device, damage the system, steal information, and enable hackers to easily access and destroy the contents of the entire system.

From a software perspective, viruses are programs or applications designed by programmers to achieve specific objectives mentioned earlier. They are programmed to gain the ability to destroy, exploit vulnerabilities, steal information, or take control of specific systems. Viruses can replicate themselves multiple times, recreate themselves, spread or attach themselves to other programs. Some of the most important types of these viruses include: (Al-Awadi, August 2016, p. 24)

4-1- The Trapdoor: This is a backdoor that is distributed when a security door is installed, giving the hacker the freedom to choose the appropriate time for the sabotage operation. This code allows access through networks while certain security systems are in place.

4-2- Hardware Virus: This type of virus generates millions of computational and consecutive input/output operations, leading to a

significant increase in the central processing unit's temperature and its burning.

4-3- Trojans: These are small programs that may be hidden within another file for camouflage. When downloaded and opened, they infect the registry and open ports, making the user's device easily vulnerable to intrusion. They are considered to be among the most intelligent programs. (Al-Awadi, August 2016, p. 24)

5- Obfuscation attacks

This involves targeting web pages and replacing them with other pages. The attacker creates a similar-looking website to the original one in order to lure and trick users into revealing their information, such as credit card details and other personal information.

6- Deceptive attacks

Deceptive attacks are carried out by exploiting the Transmission Control Protocol/Internet Protocol (TCP/IP) during the system's client-server communication. The aforementioned protocol is responsible for securing a secure connection between any two clients through port numbers and logical identity identifiers. The attacker attempts to guess the port numbers associated with data exchange and thereby impersonates the legitimate user, bypassing all protective barriers to gain access to the victim's databases. Intruders exploit protocols to manipulate network shells and redirect data to a false destination. They overload systems by inundating them with multiple messages to prevent a sender from transmitting their data. (Al-Awadi, August 2016, p. 18)

Section III: Mechanisms for achieving electronic independence in cyberspace. Conclusion: 2-the content:

To achieve electronic independence in cyberspace, it requires a set of mechanisms and measures. One of the key mechanisms is diversifying technology sources. Electronic independence relies on diversifying the technology sources used in cyberspace by avoiding complete reliance on a single technological source. Instead, competitiveness, diversity, and innovation in the technology sector should be encouraged. This can be achieved by building a strong and independent electronic infrastructure to

ensure independence in cyberspace, including developing capabilities of national networks and securing local data centers adequately.

Furthermore, enhancing awareness and providing appropriate training to the public and employees in the field of cybersecurity is essential. This contributes to raising awareness about cyber threats and enhancing the capacity to effectively and securely counter them.

A- Electronic data independence

Data independence refers to a set of standards and techniques that protect data from destruction, modification, intentional or accidental disclosure. Data security can be implemented using various methods and technologies, including administrative controls, physical security measures, logical controls, regulatory standards, and other protective techniques that restrict unauthorized user access and mitigate malicious activities.

Data security technology comes in various forms and protects data from an increasing number of threats. Many of these threats come from external sources, but organizations must also focus their efforts on protecting their data from internal threats. Methods of securing data include: (<https://n9.cl/rfdq6>.)

1- Data encryption: Applying encryption to individual data segments, granting access to encrypted data only with an authorized key.

2- Data masking: Hiding specific areas of data can protect them from disclosure to external malicious sources as well as internal employees who may misuse the data. For example, the first 12 digits of a credit card number may be masked in a database.

3- Data erasure: There are times when data that is no longer active or in use needs to be completely erased from all systems. For example, if a customer requests their name to be removed from a mailing list, the details should be permanently deleted.

4- Data resilience: By creating data backups, organizations can restore data in case it is accidentally erased, damaged, or stolen during a data breach.

B- Electronic media independence

The concept of electronic independence in the field of utilized means can be described by focusing on enhancing self-sufficiency and autonomy in the development and use of electronic technology, as follows:

1- Developing technical capabilities

This includes building local expertise and competencies in the field of designing and developing electronic means, such as software applications, database systems, and websites. By developing local technical capabilities, the country becomes less reliant on imported means and can develop customized solutions for its specific needs.

2- Building electronic infrastructure

Developing electronic infrastructure is crucial for achieving electronic independence. This includes building high-speed communication networks, data processing centers, data centers, and the necessary hardware to operate electronic services. By providing this independent infrastructure, the country can have full control over vital electronic data and services.

3- Developing local industry:

Electronic independence can be enhanced by supporting and developing local industries related to information and communication technology. Encouraging the establishment of local companies for manufacturing and supplying electronic equipment and providing related services can be encouraged. By relying on the local industry, the country can gain control over the provision and maintenance of vital electronic means.

4- Legislation and policies

Electronic independence can be promoted through the establishment of legislation and policies that encourage the use and protection of local electronic technology. These legislation and policies may include promoting research and innovation in the field of local electronic technology and providing financial support and facilitations to local companies and institutions. (Palacios, 2010, p. 03)

Section IV: The reality of electronic technology in third-world countries

Third-world countries, including African countries, did not benefit from the industrial revolution that took place in the European world. In the

18th century, these countries, especially in Africa, did not leave any imprint in terms of producing tools and technological machinery. Only a few countries, such as those in Latin America and East Asia, made some progress. However, the majority of African countries and Arab world countries remained limited to importing tools and equipment for the purpose of implementing development in their own countries. Despite entering into partnership agreements with various international organizations and regional blocs, the results of these agreements were mainly aimed at addressing developmental and economic issues to achieve high growth rates. This is due to various reasons, including a lack of resources and capabilities to invest in this sector. African countries neglected this sector and did not rely on advanced technological equipment and machinery to achieve development. For example, Arab countries establish joint industrial projects with developed countries for mere assembly purposes. Consequently, the process of technology production is almost non-existent. Most technology transfer agreements made in the past decades by developing and African countries did not focus on developing local capabilities in technology production. There are several reasons for this, including the fact that these capabilities were trained in an environment that encourages creativity and innovation, but they only found marginal and discouraging activities in their own countries in the field of scientific research, which led them to migrate to Western countries that show more interest in their talents regardless of their nationality or religion.

When technology is transferred, these countries face numerous problems imposed by industrialized countries. Conditions are imposed, considering it as their private property, exploiting the demand for financial gains only. They control its availability in the global market, and therefore, the focus is not on the benefit that developing countries can gain from it to develop their capabilities, but rather on monopolizing it to remain under their control. (Madani & Hamdi Pasha, 2013, pp. 176-177)

Section V: The impact of digital dependency on cybersecurity in African countries

When African countries purchase and import technology from abroad, they rely on foreign technology suppliers and companies. This means that the devices and software that come with this technology may have unknown security vulnerabilities or may be designed in a way that makes them susceptible to hacking and exploitation. These security vulnerabilities can be intentional or unintentional, resulting from programming errors or implicit inputs from the manufacturing companies. If these vulnerabilities are discovered by cyber attackers, they can be exploited to gain unauthorized access to state systems, networks, and sensitive data.

Furthermore, the use of imported technology by African countries can increase their dependence on foreign companies and suppliers. This creates a technological and economic dependence on foreign suppliers, meaning they may not have full control over their systems and digital technologies. This can make them vulnerable to cyber infiltration and espionage by other countries or extremist groups. Additionally, the lack of expertise, efficiency, and trained human resources in detecting and combating cyber attacks can make African countries more prone to infiltration and exploitation. (Abduladim & Al-Jawad, 2020, p. 431)

To address these challenges, African countries must enhance their capabilities in the field of cybersecurity. They should establish strict policies and procedures to ensure the security of imported technology, assess potential security vulnerabilities, and take necessary precautions to minimize the chances of cyber breaches. Training and education on cybersecurity should also be strengthened, along with fostering cooperation and partnerships with other countries and relevant international institutions in the field of cybersecurity.

In general, African countries should exercise caution when importing technology. They should work towards enhancing local capabilities in cybersecurity and developing domestic technological industries to reduce external dependence and promote technological sovereignty.

It is also important for the public sector, private sector, academic institutions, and civil society to collaborate in enhancing cybersecurity,

exchanging knowledge and expertise. Strong legislation and laws should govern the use and protection of technology and sensitive data. African countries should also have a comprehensive and integrated cybersecurity strategy that focuses on prevention, early detection, and swift response to cyber threats and how to address them.

According to the 2022 report by the Economic Commission for Africa, African cybersecurity is less mature compared to other regions, making the continent vulnerable to cyber attacks. It is expected that the African digital market will reach \$712 billion by 2050. (<https://www.worldbank.org/en/programs/cybersecurity-trust-fund/overview>) Estimates indicate that the continent loses \$4 billion annually due to cybercrime. The low level of preparedness in cybersecurity costs member states an average of 10% of their gross domestic product. This highlights the need for African governments to establish a legal and regulatory framework for cybersecurity and invest in capacity building to develop local talent.

Most African countries have attempted to introduce cybersecurity legislation. Furthermore, the continent has been facing a shortage of skilled cybersecurity professionals, estimated at 100,000 employees since 2020. This shortage is expected to increase as the e-commerce industry in Africa is projected to reach \$75 billion by 2025, according to the International Telecommunication Union. "Africa's levels of commitment to cybersecurity - as well as the ability to respond to threats - remain low compared to other continents," according to the report. (<https://www.itu.int/net4/wsis/forum/2023/ar/Agenda/Session/446>)

To support African countries in building resilience in cyberspace, the Economic Commission for Africa (ECA) has launched the Model Law Guideline on Cybersecurity for African Union Member States during the seventeenth Internet Governance Forum (IGF) held in Addis Ababa. While the guideline is not a binding law or legislation and does not seek to restrict the operation of any national or regional law, it provides a set of guiding principles that African member states may consider when developing their own cybersecurity standards to ensure security. The model guideline is

expected to provide guidance for harmonizing cross-continental electronic standards that enable African member states to take proactive measures in addressing cyber threats.

The Model Law Guideline highlighted key areas that policymakers and legal experts can explore in proposing member states to implement the Lomé Declaration through national legislative processes. It should be noted that on March 23, 2022, African heads of state and government adopted the Lomé Declaration on Cybersecurity and Combating Cybercrime in Africa to ensure that cybersecurity takes top priority at the highest level of governance.

Section VI: Mechanisms for Achieving Cybersecurity for African Countries in the Face of E-Independence Challenges

To enhance cybersecurity in African countries, it is essential to rely on a precise and comprehensive scientific approach that allows for various thinkers in different fields and sectors to reframe previous methods, techniques, and simplistic technologies. This will enable the innovation of new modes and technologies that contribute to achieving greater control over all areas of development. In the face of e-independence challenges, we can point to several mechanisms that African countries should work on and strengthen, such as:

- **Increasing awareness:** By intensifying efforts to raise awareness among users and institutions about the risks of cyber attacks and best practices for protection.
- **Developing local capabilities:** African countries are striving to enhance their local cybersecurity capabilities by training more experts and professionals in the field, establishing specialized training and research centers, and strengthening cooperation with universities and other educational institutions.
- **Enhancing regional and international cooperation:** This includes information and expertise sharing and collaboration in combating cybercrime. African countries are witnessing increased collaboration with international partners, including international organizations and major

technology companies, to enhance capabilities and exchange knowledge in cybersecurity.

- **Developing local technological industries:** African countries are actively seeking to develop local technological industries and achieve technological independence by supporting start-ups and local technological innovations, and promoting local development of cybersecurity solutions.

- **Strong legislation and laws:** African countries are working on enacting strong legislation and laws that regulate the use and protection of technology and sensitive data. A legal framework is implemented to protect cyber systems and networks and hold perpetrators of cybercrime accountable.

Despite the existing challenges, with the commitment and investment of African countries in the field of cybersecurity, greater electronic independence and enhanced cybersecurity for African nations on the Internet can be achieved. It is also important to support global efforts to enhance internet security and information technology in the African continent through international cooperation, knowledge exchange, and resource sharing with other countries.

Conclusion

Through this study, in order to achieve the necessary electronic independence in African countries, it is crucial to focus on the following key findings:

- Firstly, working towards partial independence in infrastructure, particularly in cases related to data and communication independence.
- Attempting to leverage imported technology and working towards local production.
- African countries can achieve technological independence by developing local technological industries, supporting start-ups, and promoting local technological innovations.
- Establishing research centers focused on discovering qualified local talents for the use and development of modern technology.
- The necessity of continuous training for users and institutions, integrating the public and private sectors. African governments and private companies

can collaborate in cybersecurity by exchanging information, expertise, and best practices, and implementing security measures in infrastructure and digital services.

- Raising awareness among African individuals and communities about the risks of the digital space through providing appropriate advice and guidelines and disseminating them.
- Working on establishing a legal framework that defines and regulates the use of cyberspace in African countries.

6- Bibliography

1- Books:

Erber, F. S. Technological dependence and learning revisited. Brasil: Biblioteca Digita, Iministro do desenvolvimento, industriaecomércio exterior.

Gumahad, A. T. (April 1996). Cyber Troops and Net War: The Profession of Arms in the Information Age. Maxwell AFB. War College, Air University.

Al-Awadi, A. M. (August 2016). "Cyber Information Security". Series of Publications by Al-Bayan Center for Studies and Planning.

HASSAN, f. f. An Introduction to Information Security, Defining Cyber Crimes, and How to Protect and Optimize the Available Resources to Achieve Maximum Security in the Iraqi Ministry of Interior Departments" (Ministry of Interior: General Directorate of Communications.

2 – Theses:

Bonara, Y. , "Electronic Crime," . Prince Abdul Qadir University for Islamic Sciences.

Bumflah, v. "Information Security Protection in Library Networks - A Case Study of Umm Al-Qura". Ph.D. thesis, King Abdulaziz University.

Tawilah, J. H. "Malicious Software" (Practical Guide to the Use of Malicious Software, Spyware, Prevention, and Protection Measures,). Ph.D. thesis.

3 - Journal article :

Abduladim, A., & Al-Jawad, M. (2020). cyber risks and ways to confront them in public international law. Sharia and Law Journal , 03 (35), 431.

- Craig & Others, D. (October 2014). "Defining Cybersecurity", (Technology Innovation Management Review,).
- Jubour, M. A.-A. (2012). "Cybersecurity: Challenges and Requirements for Confrontation,". League of Arab States: Arab Center for Legal and Judicial Research , 03.
- Madani, J., & Hamdi Pasha, R. (2013). the role of production and innovation of technology in the development of third world countries. New Economy Journal (09), 176-177.
- Mokhtar, M. (2015). "Cyber Security: Can Countries Avoid the Risks of Cyber Attacks?" Future Concepts Magazine. (06), 05.
- Omahi, A., & Bouadi, M. (2019). "The Role of Digital Technology in Human Resource Development (Reality and Aspirations). Notebooks of Policy and Law , 195.
- Ouissi, S., & Ghareebi, E. B. (2022). "Digital Technology and Its Impact on Individual and Social Life." Center for Scientific Research Generation. Journal of In-depth Legal Research (11), 13.
- Palacios, R. C. (2010, January). Identifying Technical Competences of IT Professionals: The Case of Software Engineers. International Journal of Human Capital and Information Technology , 03.

4 - Internet websites:

- (s.d.). Consulté le February 25, 2024, sur Op-cit: Link: [itlaw.Wikia.com/Cyber-threat](https://itlaw.wikia.com/Cyber-threat).
- <https://n9.cl/rfdq6>. (s.d.).
- <https://www.itu.int/net4/wsis/forum/2023/ar/Agenda/Session/446>. (s.d.).
- <https://www.worldbank.org/en/programs/cybersecurity-trust-fund/overview>. (s.d.).
- Jabir, S. (s.d.). "Hacking and Protection Methods,". Consulté le February 26, 2024, sur <https://download-internet-pdf-ebooks.com/4926.Free-book>
- Ramadan, K. (2019, March 21). Towards Technological Independence. Récupéré sur <https://n9.cl/5bcza0>.
- Al-Abassi, O. (s.d.). Technological Independence..The Necessity of Building National Capacities. Récupéré sur <https://www.albiladpress.com/news/2023/5531/columns/839633.html>.