The Major Challenges Facing the Development of African Countries, and Algeria in Particular, in the Face of Cybercrime

Oumeddour Radja,

University of Guelma (Guelma, Algeria)

https://doi.org/10.21684/2412-2343-2024-11-2-134-153

Abstract. The rapid development of information and communication technologies is closely related to the exponential growth in data volumes. At the same time, the development of enterprise strategies coupled with the digital economy has led to changes in business models and infrastructure solutions. The emergence of innovative industries that extensively use the internet has presented significant challenges to the security of systems and sensitive data, particularly in the field of cybercrime. In order to address the growing issue of cybercrime, African nations, among which Algeria is the largest country, need to build a series of digital barriers in the form of legislation, multilateral agreements, and the development of technical capacity in this area, such as the creation of cybersecurity centers. The implementation of an effective cybersecurity strategy is strongly required on a national, regional, and continental scale. According to the last report of the Global Cybersecurity Index 2020, Mauritius is ranked as the most secure country in Africa in terms of cybersecurity, followed by South Africa in the second rank. A successful economy inherently involves a digital economy and a bold strategy to counter all the "nuisance" of cybercrimes. Algeria, despite its relatively low ranking in the last report of the Global Cybersecurity Index, has made significant progress when compared to its neighbors. With its excellent internet connectivity and a young and dynamic population, Algeria's positive economic indicators are certain to improve even further with the desired membership it seeks in the BRICS organization. Given these considerations, it follows that South Africa as well as Algeria possess the potential to serve as locomotives for the development of the whole of Africa.

Keywords: cybercrime; cyberattack; Shodan; open ports; digital economy; South Africa; BRICS; Algeria.

Recommended citation: Oumeddour Radja, *The Major Challenges Facing the Development of African Countries, and Algeria in Particular, in the Face of Cybercrime*, 11(2) BRICS Law Journal 134–153 (2024).

Table of Contents

Introduction

This work exposes the negative impact of information technologies on the development of the digital economy. In the modern era, digital technology has brought about a wide range of comforts and conveniences, such as improved communication, access to information, and advances in medical technology, among others.[1] An important aspect of digital technology is informational technology (IT), which refers to the use of computers to process data and information. In this regard, it should be noted that at present, the potential for the prospective development of information and communication (ICT) technologies is significantly increasing because of the transition to the knowledge economy. This is one of the key factors in the development of the digital economy. The rapid development of information and communication technologies is also associated with their rapid obsolescence,

[1] *The Impact of Technology on Society: Positive and Negative Effects*, LinkedIn, 25 December 2023 (Mar. 4, 2024), available at https://www.linkedin.com/pulse/impact-technology-society-positive-negative-effects-keytech-fi.

the spread of cloud technologies and the corresponding exponential growth in data volumes, along with significant changes in the architecture and organization of computing systems. In short, the digital economy holds great promise for improving the quality of life for people. However, there is a dark side to this technology.

As technology progresses rapidly, new methods of crime also emerge. One such criminal activity is cybercrime, which occurs in the virtual world. Cybercrimes can create substantial losses for both individuals and businesses. Loss of business can also be significant in the instance of denial-of-service attacks for large corporations. For large corporations, a denial-of-service attack could result in a significant loss of revenue as well. In addition, a cyberattack could have a severe negative effect on the reputation of a company.

This study presents extensive information pertaining to cybercrime as well as explores the solutions being implemented to fight against these contemporary crimes in African countries, with a specific focus on South Africa and Algeria, which are regarded as locomotives and offer great hope for sustainable development. The expansion of internet use in African countries, and in Algeria in particular, contributes enormously to digital applications while at the same time also posing some challenges.

By the end of the 2000s, the North African countries had an information and communications network that was relatively well connected to the rest of the world. In Algeria, nearly 200,000 kilometers of fiber optic cable were deployed across the national territory at the end of 2021 as part of the national strategy to connect the country's 58 "Wilaya" (or provinces) to a state-of-the art high-speed telephone and internet network. In 2022, Algeria increased its international internet bandwidth; thus increasing the overall capacity to 7.8 Tb/s in 2022, in contrast to 2.8 Tb/s in 2021 and 1.5 Tb/s in 2020.

In recent years, Algeria has made several efforts to diversify its economy in order to ensure sustainable development. These efforts include modernizing production tools and incorporating IT solutions, all of which have contributed to good economic growth. The introduction of such modern methods management through the training of high-level executives has also earned Algeria the hope of obtaining access to the BRICS group.

1. Cybersecurity and Challenges to Improving the Digital Economy

1.1. Cybercrimes

Cybercrime, also known as computer crime, is the use of a computer for criminal purposes, such as fraud, trafficking and child pornography, identity theft, and violations of corporate and individual privacy. As the computer has become fundamental to commerce, entertainment, and e-government, cybercrime, particularly via the internet, has also increased in scope and significance. The internet has become a breeding ground for a variety of criminal activities.

Furthermore, the development of enterprise strategies, in conjunction with the digital economy, has led to significant changes in business models and the emergence of innovative solutions. Strong proficiency over the internet and expertise in using computer tools have led to a rise in cybercrimes and a growing gap between information needs, economic security, and individual freedom.[2]

Cybercrime is an umbrella term used to describe any illegal activity that involves using a computer, either as the attacker's weapon or target. This encompasses a wide variety of crimes, ranging from fishing emails and identity theft that affect individuals to ransomware and denial of service (DoS) attacks targeting businesses and organizations.[3]

The many sorts of cybercrime can be classified into three major groups, primarily crimes against people, crimes against property, and crimes against government.[4] The internet provides a discreet location for fraudulent activity and also facilitates the establishment and upkeep of cybercrime markets. Thus, the internet today is fast becoming a breeding ground for cybercriminal communities. Such a scenario, characterized by a significant increase in cybercriminal activity, has placed enormous pressure on industry participants. Substantial threats and concerns in the modern era now include ransomware and attacks on cyber-physical systems and infrastructures, such as power grids and land, sea, and air transport companies.[5]

As is generally well known, cybercrime is one of the most common activities performed by computer professionals. This work only touches on some of the effects of cybercrime. For example, cybercrime also refers to the activities perpetrated by individuals with the goal of harming organizations and stealing important data, documents, and banking information.

Considering the circumstances and the various challenges of contemporary societies, we have tried to present cybercrime or cyber criminality as a fairly widespread phenomenon. Criminality is defined as any antisocial behavior that is in direct conflict with legal and moral norms of behavior. This article examines the negative phenomenon of cybercrime as a form of criminality in contemporary society. According to research data and studies analyzed by various groups and national or international organizations, it appears that this phenomenon has become fairly widespread and poses a significant challenge in today's society. In fact, cybercrime is expanding rapidly when we take into account the interference in both official

---

2 Bejkan A. Akhmedov, *Improvement of the Digital Economy and its Significance in Higher Education in Tashkent Region*, 12 Uzbek Scholar J. 18 (2023).

3 Mercedes Cardona, *The Trend toward a Zero Trust Model for Security*, MIME CAST, 19 July 2022 (Oct. 23, 2023), available at https://www.mimecast.com/blog/the-trend-toward-a-zero-trust-model-for-security/.

4 What Are the Three Types of Cyber Crime?, Swier Law Firm (May 5, 2024), available at https://www.swierlaw.com/faqs/what-are-the-three-types-of-cyber-crimes-.cfm.

5 Trung N. Nguyen, *A Review of Cybercrime*, 2(1) J. Soc. Rev. & Dev. 1 (2023).

state and private software systems. Therefore, in addition to the positives that data digitalization and the internet provide, protective measures against piracy and hackers must also be seriously considered.

The consequences of cybercrime can be staggering following the criminal manipulation of strategic infrastructure data, or damage caused to production machines leading to reputational damage for companies, loss of productivity, loss of customers leading to a decline in revenues, and the cost of restoring business operations to normalcy. The theft of research laboratory results in high-specialized fields is also a major concern for people and companies.

Nevertheless, many countries are still faced with providing a legal doctrine that prohibits the receipt and processing of data sets. In modern research, the use of computer technology is irreplaceable. However, despite the multitude of benefits this spurt of development brings to people by improving their overall well-being, unfortunately, these great opportunities offered by computer technology are often being misused and exploited to carry out a number of crimes.

The studies conducted by different countries demonstrate their exceptional abilities in using advanced computer technology and action techniques in alignment with the development of the world economy. According to the findings of investigations, there are three main groups of people involved in computer crime, hackers, identity thefts, and cyber terrorists.[6] The following acts are all considered forms of computer activity: data theft, password theft, code theft, fraud with insurance, forgeries, violation of privacy, sabotage physical or logical, disclosure, espionage, coercion, blackmail, pornography, and propaganda.[7]

Today, it is a global problem for countries to cope with the rapid development of technology, especially when they are already faced with social changes and the objectives of meeting the needs of their populations. In order to achieve efficient protection, it is necessary to create protection strategies in accordance with international standards, introduce new norms, or update them in time. Additionally, there is a need to provide access to modern technology and professional training for the police and organizations that protect data or prevent criminal actions with adequate expertise in pursuing cybercrimes and classifying the evidence associated with these criminal offenses.

1.2. The Cost of Cybercrime

As mentioned in the previous section, the costs of cybercrime are immense and encompass a range of ramifications, such as data manipulation, theft of money, identity theft, intellectual property and personally identifiable data. Losses also

---

6 Esteban Borges, *Cybercriminals: Tactics, Impacts, and Defense Strategies*, Recorded Future, 5 February 2024 (Mar. 20, 2024), available at https://www.recordedfuture.com/threat-intelligence-101/threat-actors/cybercriminals.

7 Fitore Muqaj, *Cybercrime*, 5(11) Int'l J. Soc. Sci. Res. Rev. 456 (2022).

include the cost of tools and resources needed to cover digital forensic investigations. There have been instances in which businesses were unable to recognize malicious codes built in a complicated manner and, as a result, suffered substantial losses, had to temporarily cease commercial operations, or were forced to suspend senior executives from their jobs.[8]

Furthermore, it has been suggested that the worst is yet to come and that cybercriminal activity will pose the greatest threat to humanity over the next few decades. Cybercrimes cost approximately **$**6 trillion in losses in 2021, up nearly **$**2 trillion from 2019. According to a recent report by "Statista," the estimated annual cost of cybercrime worldwide is projected to rise from $10 trillion in 2025 to nearly $14 trillion by 2028, which is a nearly 50 percent increase.[9]

2. Internet Penetration and Vulnerability of Open Ports

2.1. Open Ports

A "port" in computer terminology refers to a virtual point where network connections start and end.[10] These points are managed by a computer's operating system, which determines the kind of services each port operates. Operating a service includes either running a process or sending and receiving data packets (units of information that are transmitted over a network, such as the internet) from other ports, such as port 443 for access through an HTTPS connection, port 80 for default access to the internet through an HTTP connection, and port 20 for data transfers. Currently, the majority of applications use predetermined port numbers assigned by the Internet Assigned Numbers Authority (IANA).[11] Open ports also have the capability to receive data packets from other ports across the internet. Some ports are reserved for specific system functions and are therefore required to be open. Closed ports, on the other hand, are unable to receive data via packets from another port and must either reject or ignore data packets. We conducted a vulnerability assessment of various open ports across Africa's cyberspace using the search engine "Shodan," an open source intelligence tool (OSINT).[12]

---

8 Ross Anderson et al., *Measuring the Cost of Cybercrime: The Economics of Information Security and Privacy*, in Conference: Proceedings of the 11th Workshop on the Economics of Information Security (WEIS) 265 (2013).

9 Anna Fleck, *Cybercrime Expected to Skyrocket in the Coming Years*, Statista, 22 February 2024 (Mar. 20, 2024), available at https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/.

10 What Is a Computer Port? Ports in Networking, Cloud Flare (Mar. 20, 2024), available at https://www.cloudflare.com/learning/network-layer/what-is-a-computer-port/.

11 Abdijabar Y. Mohamed & Samuel Kang'ara Kamau, *A Continent-Wide Assessment of Cyber Vulnerability Across Africa*, Computer Science, Cornell University 3 (2024).

12 What Is OSINT (Open Source Intelligence), Zenarmor (Mar. 20, 2024), available at https://www.zenarmor.com/docs/network-security-tutorials/what-is-osint#:~:text=The%20Shodan%20search%20engine%20allows,professionals%20and%20make%20more%20sense.

2.2. Definition of "Shodan"

During regular daily browsing of the internet, traditional search engines, commonly known as web search engines, such as Google Search and Microsoft Bing, are used by millions of people across the world to search for content on the internet. In the background, unbeknownst to the user, these search engines perform a process referred to as "crawling" the internet, where they search and index the content found during the crawling process, and render the relevant content to the user in a ranked order.[13] One such search engine is "Shodan". However, while traditional search engines, such as Google primarily search the web, Shodan's fundamental difference lies in the fact is that it is a search engine intended specifically for internet-connected devices, such as devices and servers.[14] Shodan can also be described as a "reconnaissance tool" used by cybersecurity officials, researchers, and hackers. Therefore, both ethical and malicious entities can use this platform to "crawl" the entire internet sphere and scan for IoT devices connected to the public internet.[15] Shodan is able to search for open ports across all IP (internet protocol) ranges and bypass any domestic or international bans for another country's IP ranges.[16]

Thus, for each country in North Africa, the distribution of open points by their port number was gathered using Shodan. The researchers identified each open port's functions using its port number and metadata, thereby deciphering whether it is vulnerable to attack. It was found that connected devices across Africa are highly vulnerable to attacks. According to reports, three of the most commonly open ports that devices across Africa use have serious documented vulnerabilities.[17] Additionally, the findings indicate that 69.8 percent of the devices with one of the five commonly used open ports are vulnerable to cyberattacks.[18]

This information enables the researchers to analyze how vulnerable each country is to attack. Unauthorized access to an open port in one country also poses the grave risk of leading to security vulnerabilities in other countries.[19]

The current ranking of cyber vulnerabilities is based on a simple probabilistic model, where a higher number of open ports implies a higher number of attack

---

13 Mohammed & Kamau 2024, at 3.

14 What Is Shodan, Shodan Help Center (Mar. 20, 2024), available at https://help.shodan.io/the-basics/what-is-shodan.

15 Mohammed & Kamau 2024, at 3.

16 John Matherly, *Complete Guide to Shodan: Collect. Analyze. Visualize. Make Internet Intelligence Work for You* (2016); Mohammed & Kamau 2024.

17 Mohammed & Kamau 2024, at 4.

18 *Id.*

19 Mohammed F. Abdulqader, *Penetration Testing on FTP Server*, 5(12) Int'l J. Enhanced Res. in Sci. Tech. & Engineering (2016) (Mar. 20, 2024), available at https://www.researchgate.net/publication/324390613_Penetration_Testing_on_FTP_Server.

vectors for cybercriminals. As a result, a higher number of attack vectors essentially means a greater likelihood of cybercriminals gaining unauthorized access.[20]

Before proceeding to the rest of the research, it appeared thus logical to introduce the concept of ports and Shodan.

2.3. Most Vulnerable African Countries by Open Internet Ports

Let us now examine some data pertaining to the vulnerability of African countries in terms of cyberattacks, with a specific focus on the number of open internet ports in these countries and their susceptibility to attacks. As the internet penetration rate in Africa increases, so does the proliferation of internet of things (IoT) devices. Along with this growth in internet access comes the risk of cyberattacks on vulnerable IoT devices mushrooming in African cyberspace.[21]

The data used in the tables that follow comes from a study conducted on the distribution of open ports in various African countries. An effective method for identifying vulnerabilities in IoT devices is to first locate open ports. Thus, the Shodan platform was extensively used to identify the most commonly used open internet ports in African cyberspace and determine their vulnerability to cyberattacks.[22] According to the data presented in Table 1 below, three of the five most commonly used open ports were found to be particularly susceptible to attacks.

Table 1: **Most vulnerable open internet ports in Africa**[23]

Port number	Open port count
7547	943,126
80	845,660
443	567.844
22	303,406
53	227,144
21	222,144
23	220,393
2000	173,782
123	126,557
8291	94,056

[20] Leona McNulty, *IoT Vulnerability Assessment of the Irish IP Address Space*, F5, 17 November 2020 (Mar. 20, 2024), available at https://www.f5.com/labs/articles/threat-intelligence-/iot-vulnerability-assessment-of-the-irish-ip-adress-space.

[21] Mohammed & Kamau 2024, at 1.

[22] *Id.*

[23] Lyndon Sutherland, *Mirai Evolving: New Attacks Reveals Use of Port 7547*, Security Intelligence, 1 December 2016 (Mar. 20, 2024), available at https://securityintelligence.com/mirai-evolving-new-attack-reveals-use-of-port-7547/.

The collected data was then used to ascertain the number of open ports that were most frequently used in each country in Africa. These ports were ranked on the basis of their degree of vulnerability to cyberattacks, from most vulnerable to least vulnerable. It was found that Tunisia, Morocco, Egypt, Algeria, and South Africa have the highest number of commonly used open internet ports that have been proven to have documented vulnerabilities (Table 2 below).[24]

Table 2**: Most vulnerable African countries by open internet ports**

Countries	Open port counts
South Africa	2,398,737
Tunisia	1,088,758
Morocco	559,383
Egypt	476,233
Nigeria	191,148
Kenya	155,333
Algeria	111,712
Mauritius	95,704
Libya	30,105

Thus, by analyzing all of the collected data, the researchers were able to compare the vulnerability of different countries in Africa to cyberattacks. Through the utilization of open source intelligence tools, it was discovered that a significant number of the most commonly open ports on devices are highly susceptible to being compromised. These vulnerabilities can be exploited by cybercriminals to gain unauthorized access to systems, plant malware into devices, and cause service disruptions to organizations by launching distributed denial of service (DDoS) attacks.[25] Furthermore, criminals can also gain unauthorized access to systems by exploiting vulnerabilities in open ports that are listening for service.

Based on the findings of this research, it is recommended that internet service providers (ISPs) establish policies that prioritize the adoption of key considerations, including implementing additional security protocols and port hardening, ensuring software continuity, guiding users to follow best practices, and conducting regular network and system audits.

Following these analyses, definitive conclusions have been established, along with policy recommendations for both the public and private sectors. However, despite the high stakes involved, there is still a lack of adequate research on the nature of vulnerable IoT's that remain exposed to the public internet.

[24] Mohammed & Kamau 2024, at 1.

[25] *Id.* at 4.

3. Cybersecurity in Africa

3.1. World Internet Users in Africa

The ability to regulate information on the internet is crucial in combating the growth of cybercrimes and addressing the growing gap between the need for information, economic security, and individual freedom. The following paragraphs present some information about the population and internet access in Africa.

Population of Africa: 1,394,588,547 people
Population percentage of world: 17.6%
Number of internet users: 601,940,784 users
Penetration rate: 43.2%
Growth change percentage: 2000–2023: 13.233%
Global internet penetration rate: 11.2%

Despite technology remaining a bottleneck in its industrialization efforts, the African continent, home to approximately 1.4 billion people, is said to be on the cusp of colossal changes as the next frontier of the transformative digital boom. According to Internet World Stats estimations, as of 31 December 2021, Africa had 590.3 million internet users. This corresponds to an internet penetration rate of 43 percent and a growth of 12.975 percent from 2000 to 2021.[26] The corollary of an increased internet penetration rate is the rapid proliferation of IoT devices in smart homes and critical infrastructures, such as military applications, Industrial Control Systems (ICS), hospitals, and financial institutions. Nevertheless, the promise of a digital Africa has a sordid underbelly: each year, African economies lose millions of dollars to cybercrime.[27]

According to the data available, Africa exhibits low internet connectivity in several countries throughout the continent, as well as significant disparities between these countries. For instance, with the exception of South Africa and a few countries in North Africa, the majority of the countries in the Sahel and central African regions are poorly connected. The situation in Africa is marked by a significant delay in economic development, particularly in the realm of the digital economy. However, there is hope for many African countries, particularly those that are currently experiencing high growth rates, to achieve sustainable development in the future.[28]

In Algeria, nearly 200,000 kilometers of fiber optic cable had been installed across the national territory at the end of 2021, as part of the national strategy to connect the country's 58 "Wilaya" to state-of-the art high-speed telephone and internet

---

[26] Internet and World Stats, Usage and Population Statistics (Mar. 20, 2024), available at https://www.internetworldstats.com/africa.htm.

[27] Mohammed & Kamau 2024, at 1.

[28] Internet and World Stats, Usage and Population Statistics (Mar. 20, 2024), available at http://www.internetworldstats.co/stats.htm.

network. In 2022, Algeria increased its international internet bandwidth, thereby increasing its overall capacity to 7.8 Tb/s.

Top 10 countries with the best internet connectivity in Africa in 2021:
1. Algeria.
2. Morocco.
3. Nigeria.
4. South Africa.
5. Namibia.
6. Cameroon.
7. Cote d'Ivoire.
8. Egypt.
9. Senegal.
10. Tunisia.

3.2. Internet Connectivity in Africa and Major Challenges

In today's world, there is a growing dependence on modern technology, with a country's digital quality of life having an enormous effect on people's daily lives. The Digital Quality of Life Index (or DQL Index) assesses the state of digital well-being in numerous countries throughout the world. The study indexes each country according to five criteria pillars that affect a population's overall quality of life, namely internet affordability, internet quality, electronic infrastructure, electronic security, and electronic government.[29] According to a comprehensive study conducted in 2022 across 117 countries using the DQL Index, South Africa had the highest rating for quality of life with nearly 0.41 points, followed closely by Mauritius and Morocco (Table 3 below).

Table 3: **2022 Digital Quality of Life Index (DQL Index) of African countries**

Countries	DQL Index	Global Rank	Rank in Africa
South Africa	0.4131	66	1
Mauritius	0.4117	68	2
Morocco	0.4051	71	3
Tunisia	0.3848	77	4
Kenya	0.3836	78	5
Egypt	0.3475	85	6
Nigeria	0.3437	86	7
Ghana	0.3300	88	8
Algeria	0.3222	92	9
Senegal	0.3143	95	10

[29] Digital Quality of Life Index (DQL Index) (Mar. 20, 2024), available at https://surfshark.com/dql2022.

Although many African nations recognize the importance of safeguarding and improving their country's critical infrastructure from cyber threats, unsurprisingly, African countries are lagging behind on these issues. While Europe and North America are among the top-ranked countries in the index, Asia and South America show a more mixed picture, with some countries leading the way and others falling short. In Africa, Mauritius takes first place, followed by Rwanda in second and Kenya in third. Despite the fact that over the past decade, the African continent has made great strides in developing the necessary information and communication technology infrastructure, only four countries, notably South Africa, Kenya, Uganda, and Rwanda, have a cyber-security strategy. Additionally, only a handful of countries have legislation specifically addressing cybercrime, which includes provisions pertaining to global collaboration in the fight against cybercrime.[30]

An essential objective outlined in any national cybersecurity strategy is to bolster international collaboration through ratification of international conventions on cybercrime (such as the Budapest and Malabo Conventions) and continued participation in regional and international initiatives. The Budapest Convention was the world's first international treaty addressing internet and computer crimes by harmonizing national laws and increasing cooperation between nations. Although it is a Council of Europe Convention, several non-member states of the Council of Europe were actively involved in the adoption of the Convention, and it is now open for ratification or accession by all countries.

After the 23rd African Union held in Malabo on 26–27 June 2014, the African Union Convention on Cybersecurity and Personal Data Protection adopted a legal framework for addressing cybercrime and data protection, which is referred to as the Malabo Convention.

South Africa is among the top-ranked African countries in terms of cybersecurity. Thus, in March 2019, in order to reinforce its cybersecurity strategy, the South African Parliament passed what is called "critical infrastructure legislation." This legislation aims to enable the identification and designation of certain facilities as critical infrastructure and provide the criteria necessary for assessing the protection, preservation, and resilience of such critical infrastructure.

Although South Africa, Algeria, and a few other African countries have made attempts and implemented steps in the right direction in response to cybercrime, only a limited number of countries have actually enacted laws that are necessary to safeguard consumers and enterprises. According to the Global Cybersecurity Index (2021), out of the 54 African countries evaluated, only 29 had implemented cybersecurity laws.[31]

---

30 Cybersecurity, Cybercrime and Child Protection in Africa: National Approaches and Elements of Foreign Policy, Diplo (Mar. 20, 2024), available at https://www.diplomacy.edu/resource/report-stronger-digital-voices-from-africa/cybersecurity-cybercrime-cop-in-africa-national-approaches/#:~:text=Many%20African%20countries%20%E2%80%93%2039%20in,international%20cooperation%20in%20tackling%20cybercrime.

31 Shane McCarthy, *Africa Must Act Now to Address Cybersecurity Threats: Here's Why*, World Economic Forum, 17 August 2020 (May 7, 2024) (Mar. 20, 2024), available at https://www.weforum.org/

A majority of businesses in Africa, more specifically 52 percent, expressed a lack of preparedness in dealing with a major cyber assault. The actual situation is even bleaker; according to Interpol's "African Cyberthreat Assessment Report," over 90 percent of enterprises across the continent were functioning without the essential cybersecurity protocols.[32]

Table 4 below presents the African countries that are considered the most secure in terms of cybersecurity, according to the current Global Cybersecurity Index from the International Telecommunication Union (ITU). The ITU index evaluates the growth of each country based on the five strategic pillars, namely legal measures, technical measures, organizational measures, capacity building, and international cooperation. Mauritius achieved the highest position in Africa, yet it ranked 17th on the global scale. Tunisia and Ghana followed Egypt as the second-ranked country in Africa.[33]

Table 4: **Ranking of North African countries in terms of cybersecurity according to the ITU Global Cybersecurity Index 2020**[34]

Country	Overall score	Legal Measures	Technical Measures	Organizational Measures	Capacity development	Cooperative Measures
Egypt	95.48	20.00	17.45	20.00	19.12	18.91
Tunisia	86.23	20.00	19.54	12.21	16.96	17.52
Morocco	82.41	18.40	17.94	12.37	15.24	18.46
Algeria	33.95	12.46	02.73	01.44	10.07	07.25
Libya	28.78	0.73	08.54	03.13	05.34	08.04
Mauritania	18.94	12.55	00.00	06.39	00.00	00.00

agenda/2022/08/africa-must-act-to-address-cybersecurity-threats/; INTERPOL, *Interpol African Cyberthreat Assessment Report 2024* (3rd ed., April 2024) (May 2, 2024), available at https://www.interpol.int/content/download/21048/file/24COM005030-AJFOC_Africa%20Cyberthreat%20Assessment%20Report_2024_complet.pdf.

32 *Id.*

33 Top 10 African countries with the best cybersecurity revealed, Security and Fire Africa (Mar. 20, 2024), available at https://securityafricamagazine.com/top-10-african-countries-with-the-best-cybersecurity-revealed/.

34 Global Cybersecurity Index 2020: Profile of African Countries, from Source ITU Global Cybersecurity Index v4 (2020) (Mar. 20, 2024), available at https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E.

Table 5: **Global Cybersecurity Index 2020: per country profile of African countries**[35]

Country	Overall score	Legal measures	Technical measures	Organizational measures	Capacity development	Cooperative measures
Mauritius	96.89	19.27	20.00	18.38	19.54	19.70
Tanzania	90.58	18.54	18.31	16.60	17.72	19.41
Egypt	95.48	20.00	17.45	20.00	19.12	18.91
Ghana	86.69	19.35	18.48	17.78	15.44	15.63
Tunisia	86.23	20.00	19.54	12.21	16.96	17.52
Nigeria	84.76	20	17.09	18.98	12.21	16.48
Morocco	82.41	18.40	17.94	12.37	15.24	18.46
Kenya	81.70	20.00	18.27	12.75	14.78	15.89
Benin	80.06	17.42	13.94	19.48	13.60	19.70
Rwanda	79.95	20.00	13.0	16.83	16.3	13.82
South Africa	78.46	16.82	15.85	12.50	13.60	15.63

To effectively combat cybercrime, African countries including Algeria must promote the development of technical expertise through the creation of research centers specializing in cybersecurity and ensure good quality training for judicial resources. Furthermore, in an effort to improve cooperation with international institutions, it is necessary to move forward from the phase of addressing issues at the local level, by establishing cooperation mechanisms at the continental and global levels while ensuring to harmonization of legal laws and regulations.

4. Algerian Regulation and Judicial Training on Electronic Evidence and Cybercrime

4.1. Reinforcement of Legislation against Cybercrimes in Algeria

In 2015, the Algerian government officially established a National Authority with the objective of preventing and combating infringements related to information and communication technology. This authority is also known as the Center for the Prevention and Fight against Computer Crime and Cybercrime (CPLCIC). According to a decree published in the official journal on 8 October 2015, this new authority was put under the responsibility of the Ministry of Justice.

35 Global Cybersecurity Index 2020, supra note 34.

Even though it is true that a law specifically addressing cybercrime is still lacking in Algeria, it has been revealed that proposed laws on the subject are being finalized, highlighting the need for adapting and updating Algerian legislation to developments in the world.

Moreover, in order to fight this type of contemporary crime, the Algerian legislator promulgated a set of texts, including amendments, to the Algerian penal code and the Law No 09-04 of 2009, which provide regulations for preventing and combating offenses related to information technology, and communication. The law cited above was followed by the Law the No. 16-2 of 2016, which updated to complete the legal arsenal.[36]

Furthermore, a specialized workshop on advanced judicial training on cybercrime investigations and electronic evidence was organized in Algiers from 3–6 December 2018, which was dedicated to the magistrates who had successfully completed the required training.

Moreover, in order to fight this type of contemporary crime, the Algerian legislator promulgated a set of texts, including amendments, to the Algerian penal code and the Law of 09-04, which provide regulations for preventing and combating offenses related to information technology, and communication. This was followed by Law No. 16-2 of 2016, which updated the code to criminalize the use of information technologies and communication to engage in terrorist acts; Law No. 18-7 related to the protection of individuals during the processing of personal data; and Presidential Decree No. 20-05 of 2020.

In order to be in harmony with world developments, the Algerian legislator has established a specialized national penal code that is specifically dedicated to combating crimes related to information and communication technologies, as well as other related crimes affecting state security or national defense.

The Algerian legislator stipulates that there is established, near the court of Algiers, a specialized national penal unit, responsible for the prosecution and investigation of offenses linked to information technologies and of communication and related offenses.

It is also competent to judge violations that constitute crimes, offenses related to information and communication technologies of great complexity; within the meaning of this code, are included any offense committed or whose commission is facilitated by the use of a computer system or an communication electronic system, or any other method or process linked to information and communication technologies.

It includes:

• offenses affecting state security and national defense;

---

[36] Oumeddour Radja & Fercha Kamel, *Penal Inspection in the Virtual Environment*, 7(1) ASJP 973 (2020) (Mar. 20, 2024), also available at https://www.asjp.cerist.dz/en/article/117094.

• offenses relating to the dissemination and propagation, in the public, of misleading information likely to undermine public security and peace or the stability of society;

• offenses affecting the automated data processing systems of public administrations and institutions;

• the offenses of human trafficking, human organ trafficking and migrant smuggling;

• offenses of discrimination and hate speech.

It also includes:

• the most complex crimes that are considered based on the number of perpetrators, co-perpetrators, or those affected, because of the wide geographical area of the place where the crime was committed. It encompasses the seriousness of its effects, or the damages resulting from it, or because of its organized or transnational nature, or its violation of public order and security, as it requires the use of special investigative means or specialized technical expertise or resorting to international judicial cooperation.[37]

Following these efforts, Algerian authorities have also expressed interest in adopting and implementing new legislation with the support of the judicial institutions of the Council of Europe in 2022. At the international level, Algeria has moved up to an intermediate position among the 192 countries that were included in the Global Cybersecurity Index for 2020. In this regard, Algeria ranks 23rd in Africa. Notwithstanding this ranking, compared to its neighbors, Algeria has made a lot of progress, as has the awareness of the Algerian legislator.

However, as stated, it is necessary to proceed forward from the phase of developing local and regional regulations, such as by creating a specialized center and encouraging the training of the necessary human resources. Greater efforts must be made to improve the Algerian communication system, taking into account the five parameters included in the evaluation of the Global Cybersecurity Report, for a better ranking among emerging countries.

4.2. Algeria's Application for Membership in the BRICS Organization

Algeria has witnessed a resurgence of economic growth following the restoration of political stability in 2020 and the disappearance of the negative effects linked to the COVID-19 pandemic. Economic indicators for 2022, 2023, and the forecasts for 2024 reveal a growth rate of well over 4.5 percent.

Furthermore, Algeria, a member of the Organization of Petroleum Exporting Countries (OPEC) and an important producer and supplier of gas and oil, is actively pursuing the diversification of its economy. The country's exports, excluding

[37] Article 211 bis 22 to bis 25, order 21-11 of 25 August 2021 supplementing order 66-155 of 8 June 1966 on the Code of Criminal Procedure, Official Journal of the Algerian Republic, No. 65, 26 August 2021, p. 8.

hydrocarbons, have shown a clear progression, from $5 billion in 2021 to $7 billion in 2022 and $10 billion in 2023.

This significant improvement in the Algerian economy, along with an almost zero external debt, will permit Algeria to improve all the indexes cited above in the next few years.

On 7 November 2022, Algeria announced the submission of its application for membership in the BRICS organization. However, in order to have the desired impact on this group, Algeria must intensify its commitment to digital development and new technologies.

With a young and qualified workforce, close proximity to Europe and strong ties with BRICS members, the country holds considerable opportunities for global economic integration.

Algeria's ambition to become a member of the BRICS group motivates it to intensify exchanges and cooperation in all economic and political areas with the aim of building a better future on bilateral and multilateral levels with the BRICS countries. This will also facilitate the establishment of a stronger future relationship with the BRICS countries, with whom it already maintains excellent relations. Algeria's contribution to the process of establishing a multipolar world is expected to only be further strengthened as a result of this association.

Table 6: **Comparison between South Africa and Algeria in terms of economic growth and cybersecurity parameters**

Parameters	**South Africa**	**Algeria**
Population 2023	61 millions	45 millions
GDP (PPP) **$** estimate	999 billion 16,630	629 billion 13,681
GDP (nominal) **$** estimate	401 billion 6,430	224 billion 4,874
Internet domain	.za	.dz
Overall score for cybersecurity	78.46	33.95
Legal measures	16.82	12.46
Technical measures	15.85	02.73
Organizational measures	15.85	01.44
Capacity development	13.60	10.07
Cooperative measures	15.63	07.25

As we conclude this section, it is important to note that Algeria's ranking in the last Global Cybersecurity Index 2020 report,[38] was unfavorable as shown in Table 6 above. These evaluations are truly surprising, with one plausible explanation being the effects of political turmoil that transpired in Algeria in 2019, which resulted in erroneous conclusions. However, this not only mitigates but also fails to accurately reflect the great progress made in recent years.

Conclusion

Cybercrime is currently one of the major issues facing African countries as well as entire states worldwide. Upholding the safety and security of the internet is the responsibility of law enforcement agencies. In order to effectively detect, prevent, and respond to cybercrime, it is imperative that these authorities introduce and implement globally applicable new techniques and talents.

As part of its efforts to combat cybercrime, Algeria has enacted a number of cyber laws. These laws are designed to safeguard Algerian citizens and organizations. The economic indicators in Algeria are all green following the restoration of political stability and the resumption of economic growth. Its performances are expected to improve even further in the immediate future on economic, social, and scientific levels, which will allow Algeria to concretize its prospects of joining the BRICS alliance.

However, it is necessary to move forward from the phase of developing policies at the local level by creating a specialized center and encouraging the training of the necessary judicial and legal resources. The quality of training and research in the field of cybersecurity should be improved, and at the same time, legal documents should be brought up to date and standardized in order to facilitate improved collaboration with international organizations. A successful economy invariably involves a proactive digital economy and an efficient strategy in order to effectively counter all the "nuisance" of cybercrime. Currently, several countries in North Africa have adopted national cybersecurity strategies. Establishing a regional union similar to the Maghreb Union or Arab League, which would unify Arab and continental cybersecurity policy frameworks under a common body such as the African Union, would go a long way in providing guidance to entities operating in Africa regarding the baseline standards for setting up their systems and handling user data.

According to the report of the Global Cybersecurity Index 2020, Mauritius ranks as the top African country in terms of cybersecurity, followed by South Africa. However, regardless of its ranking relative to its neighbors, Algeria has made significant progress in the last two years, and these indicators will certainly improve further with the desired membership of Algeria in the BRICS organization. Due to the great

[38] Global Cybersecurity Index 2020, *supra* note 34.

potential for development in Africa, particularly in the areas in which the digital economy plays a major role, this study can also serve as an assessment tool for the expansion and intensification of direct investment in Africa in general and in Algeria in particular.

With a wealth of natural resources, modern infrastructure, a high economic growth rate, a young and dynamic population, quality training for its executives, and up-to-date legislation, Algeria aims to contribute fully to the BRICS organization, with which it maintains strategic and privileged relationships. By initiating significant investment initiatives and using every opportunity to establish themselves as industry leaders, Algeria is already paving the path to becoming future frontrunners in this rapidly changing global landscape.

Acknowledgments

I declare that I have no known competing financial interests or personal relationships that could have appeared to influence the work presented in this manuscript. This work was carried out on a personal level, independently of my thesis work, and without any funding from any organization or institution.

I would like to thank the two anonymous reviewers who invested their valuable time in providing eventual comments or suggestions to improve the manuscript.

References

Abdulqader M.F. *Penetration Testing on FTP Server*, 5(12) International Journal of Enhanced Research in Science, Technology and Engineering (2016).

Akhmedov B.A. *Improvement of the Digital Economy and its Significance in Higher Education in Tashkent Region*, 12 Uzbek Scholar Journal 18 (2023).

Anderson R. et al. *Measuring the Cost of Cybercrime: The Economics of Information Security and Privacy*, in Conference: Proceedings of the 11th Workshop on the Economics of Information Security (WEIS) 265 (2013). http://dx.doi.org/10.1007/978-3-642-39498-0_12

Gordon S. & Ford R. *On the Definition and Classification of Cybercrime*, 2(1) Journal of Computer Virology 13 (2006).

Matherly J. *Complete Guide to Shodan: Collect. Analyze. Visualize. Make Internet Intelligence Work for You* (2016).

Mohammed A.Y. & Kamau S.K. *A Continent-Wide Assessment of Cyber Vulnerability Across Africa*, Computer Science, Cornell University 3 (2024). https://doi.org/10.48550/arXiv.2301.03008

Muqaj F. *Cybercrime*, 5(11) International Journal of Social Science Research and Review 456 (2022). http://dx.doi.org/10.4781/ijssrr.v5i11.789.

Nguyen T.N. *A Review of Cybercrime*, 2(1) Journal of Social Review and Development 1 (2023).

Radja O. & Kamel F. *Penal Inspection in the Virtual Environment*, 7(1) Algerian Scientific Journal Platform 973 (2020).

Information about the author

Oumeddour Radja (Guelma, Algeria) – Assistant Professor, Department of Law, Laboratory of Environmental Legal Studies, Faculty of Law and Political Science, University of Guelma (Guelma, 24000, Algeria; e-mail: radja-oumeddour@hotmail.fr; oumeddour.radja@univ-guelma.dz).