JOURNAL OF SECURITY AND SUSTAINABILITY ISSUES
ISSN 2029-7017 print/ISSN 2029-7025 online
2023 Volume 13
https://doi.org/10.47459/jssi.2023.13.6

CYBERSECURITY IN ALGERIA

Zoltán Sipos

Óbudai University, Doctoral School for Safety and Security Sciences,
H-1081 Budapest, Népszínház utca 8., Hungary

Received 17 January 2023; accepted 13 March 2023; published 30 March 2023

Abstract. Cybersecurity is an important issue for individuals, organizations, and governments in Algeria and around the world. Cyberattacks can have serious consequences, including financial loss, theft of sensitive information, damage to reputation, and disruption of essential services. To help protect against these types of threats, it is important for individuals and organizations to take steps to secure their systems and data. This can include using strong passwords, keeping software and security protocols up to date, and being cautious when interacting with unfamiliar websites or individuals online. Governments may also have policies and regulations in place to help protect against cyber threats and to respond to incidents when they do occur. Algeria is currently not among the countries that prioritize cyber security sufficiently.

Keywords: cyber security; Algeria; threat

Reference to this paper should be made as follows: Sipos, Z. 2023. Cybersecurity in Algeria. *Journal of Security and Sustainability Issues*, 13, 65-73. https://doi.org/10.47459/jssi.2023.13.6

JEL Classifications: O55

1. Introduction

The People's Democratic Republic of Algeria, which is bordered by six North African countries, is the second-largest country in terms of land area in the world and the second-largest on the African continent (Turianski, 2020). Its territory has been plagued by terrorism for ten years, making it difficult for the Algerian government to strike a balance between combating extremism and growing the country's economy.

Both the public and private sectors are extremely susceptible to cybercrimes (Kovács, 2022). Sub-Saharan African banks are particularly susceptible to cyberattacks (MacGibbon, 2015), according to Dataprotect, a data security firm with headquarters in Morocco. This is mostly because of a shortage of experienced experts and a lack of investment in cybersecurity. This is clearly demonstrated by the fact that several countries on the African continent have experienced successful hacker attacks targeting against critical infrastructures including healthcare institutions and systems (Besenyő, Márton & Shaffer, 2021).

A survey of 21 banks in West and Central Africa conducted in 2020 found that more than 85% had previously experienced at least one cyber-attack. A third of these attacks used phishing, while over 30% involved bank card fraud (Mitchell, 2022). On March 11, 2022, the Ministry of Justice's official Twitter account was hacked, according to the official Algerian radio. According to official sources Moroccan hackers were responsible for the posts that had nothing to do with the Algeria's foreign policy. This proved that there are further conflicts waging in cyberspace, referred to by some experts as a "shadow war," in addition to the political difficulties between Algeria and Morocco.[1]

Hackers took control of the Ministry of Justice's official Twitter account and posted a number of messages in support of Russia's intervention in Ukraine, accusing Ukrainian President Volodymyr Zelensky of "Naziism and the slaughter of his compatriots." On March 12th, the Algerian Judicial

Council opened a judicial investigation in connection with the hacking, promising that "the public will be notified of the investigations' findings in a timely way."

Cyberattacks are not a new phenomenon (Falg & Kovalčíková, 2022). The General Confederation of Moroccan Enterprises (CGEM) website was breached in November 2021, and the Algerian Ministry of Finance's website was attacked by the Moroccan hacking group called "Morocco Hack Team". Despite Morocco's denial of the Algerian claims, the Moroccan daily Hespress published information on Moroccan hackers' hacking of dozens of websites linked to Algerian government sectors on February 16, 2021 (Dessi, 2011).

These conflicts are a result of the long-running disagreement over Moroccan sovereignty over Western Sahara. Cyberattacks are now a frequent strategy in disputes and conflicts on a worldwide scale. The recent cyberattacks between Morocco and Algeria could be seen as a new development in an unconventional battle. Enemies have a greater window of opportunity to attack on hinterland because key infrastructure is susceptible to cyberattacks potentially crippling and disrupting important military, security, and economic sectors. (Ramluckan & Niekerk, 2020). Given Algeria's repeated claims that Morocco is using cyberwarfare, several experts argue that the country's leadership is pursuing internal political objectives. It attempts to persuade Algerians that their country is at war with Morocco, a "foreign opponent," in an effort to quiet calls for widespread protests (Bashir, 2022).

In keeping with the back-and-forth attacks of recent years, an Algerian hacker targeted the official website of the Moroccan Dhar El Mahraz Science University in Fez in August 2022, while earlier the General Confederation of Moroccan Enterprises (CGEM) in Morocco was the target of a cyberattack in November 2021. (FSDM). Even while the cyber operations don't seem to have been carried out solely for political reasons, tensions between the two nations were high at the time. Algeria chose to sever ties with Morocco in August 2021 after charging Rabat of compromising national security, particularly online. Morocco refuted the charges (Kasraoiu, 2022).

Despite the fact that the region's cyber security leaves plenty to be desired (Ndemo, 2021), there are projects of a certain sort that help to enhance security, such as the following:

- Project CyberSouth, a joint initiative of the EU and the Council of Europe (2017–2020), aims to strengthen institutional and legislative capacities on cybercrime and electronic evidence in the Southern Neighborhood region in accordance with requirements for respect for human rights and the rule of law. The project's priority nations are Algeria, Jordan, Lebanon, Morocco, and Tunisia. (Project CyberSouth, 2017),
- Allows parties to develop a single criminal strategy aimed at defending the Arab society against information technology offenses. Arab Convention on Combating Information Technology Offenses (League of Arab States General Secretariat, 2012),
- U.S. Algeria aims to modernize its security sector, improve security collaboration and information sharing with regional and international partners, and reduce dependence on Chinese and Russian equipment and technology through increased engagement with U.S. counterparts to fight cybercrime, terrorism-financing, and develop security-related capacity (Integrated Country Strategy, 2022).

[1] Morocco and Algeria have been fighting for the leading role within the Maghreb region for decades. In October 1963, a short border war broke out between the two countries (Sand War), which ended with a peace treaty in February 1964. The two countries also take opposite positions regarding the former Spanish colony, Western Sahara. Algeria supports the Sahrawis fighting for independence, and Morocco is willing to grant only limited autonomy to the occupied territories. In 2021, another armed conflict broke out between the Polisario Front and Morocco, in which Algeria does not take part, but provides shelter to the exiled Sahrawi government. More on this: János Besenyő: Western-Sahara under the Spanish empire, AARMS, Volume 9, Issue 2. 2010, pp. 195-215; János Besenyő, Marcell György Pintér: The MINURSO Police Contingent, In: János, Besenyő; Joseph, Huddleston; Yahia, H. Zoubir (eds.) Conflict and Peace in Western Sahara: The Role of the UN's Peacekeeping Mission (MINURSO), Routledge, CRC Press (2023), 368 p. p 193.

2. Case study of an Algerian hacker

In spite of the fact that Algeria is not a leader in the field of cyber security, the Trojan horse that was created by Hamza Bendelladj, who was 27 years old at the time, made quite a stir in the early 2000s.

It is believed that Bendelladj was one of the co-creators of the banking Trojan known as "SpyEye", which is believed to have infected around 1.4 million computers in the United States between the years 2009 and 2011. Users could potentially extort other users by using the software to obtain login information for online bank accounts and then using that information to blackmail other users.

According to the United States Department of Justice, Bendelladj entered a guilty plea, for which he was punished with a jail sentence of thirty years and an order to pay fourteen million dollars in reparations. Following a two-year manhunt in Thailand, Bendelladj, also known as the "happy hacker," was arrested in 2013 and deported to the United States from that country.

The fact that he was photographed smiling during his arrest led to him being given the nickname "happy hacker." It is believed that he sold the data stolen by the virus on an underground internet marketplace. Although the court filings do not clarify what happened to the money, numerous online stories claim that Bendelladj used it to fund various Palestinian charities, turning him into a hero in the eyes of many individuals (U.S. Attorney's Office, 2013).

3. Defence infrastructure and legislative framework

Even though the continent of Africa still faces numerous difficulties, such as poverty and political unrest, its economy has expanded significantly in the recent years. Many nations have recovered quickly from pandemics because of rising digital technology usage and consumption at the local level. While these technologies have accelerated expansion, they have also raised issues with cyber security. African companies are a preferred target for cyber criminals, according to study (KPMG, 2022).

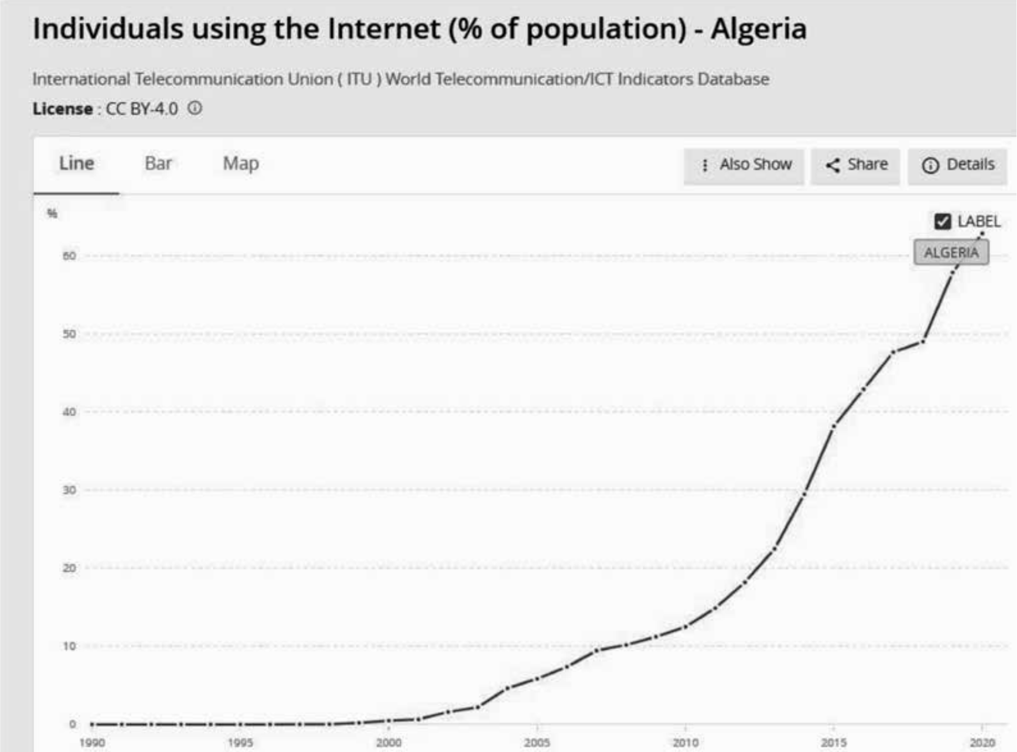
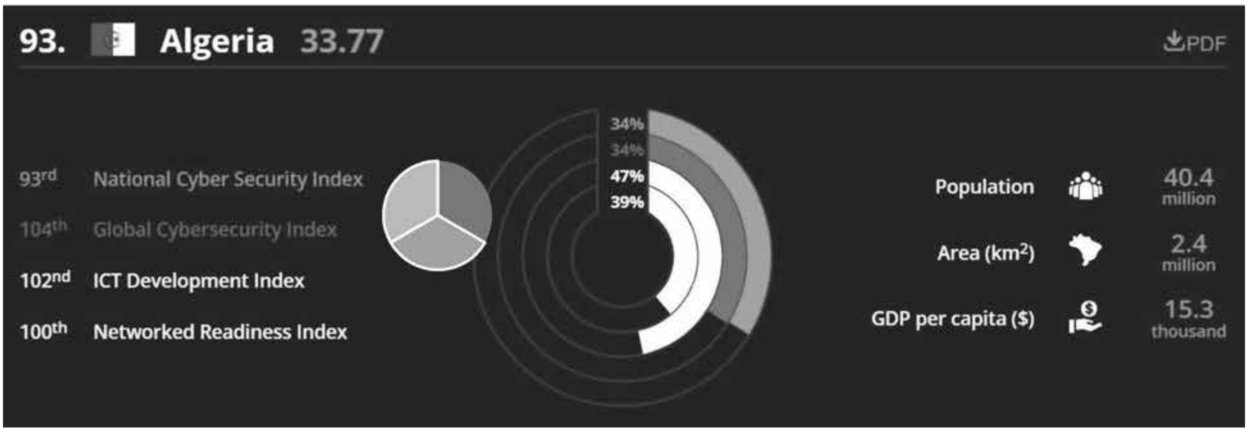


Figure 1. The World Bank - Individuals using the Internet (% of population) – Algeria

Source: https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=DZ

Figure 1 depicts the use of the internet by individuals between 1990 and 2020. Over the course of 30 years, the number of users increased by 60%. In a global comparison, Algeria comes in 145th with an average download speed of 10.91 Mbit/s for fixed-network broadband internet. Only 0.79 Mbit/second was the upload rate, which was much less (180th place). Algeria ranks 123rd in terms of download speed for mobile internet, which includes tablets and smartphones, with a rate of 13.71 Mbit/s. The upload speed of around 11 Mbit was sufficient to rank 63rd (WorldData.info).

Algeria ranks lower than average on both the National Cybersecurity Index (93rd) and the Global Cybersecurity Index (104th), two reliable indicators of how committed nations are to cybersecurity on a global scale (NCSI). (See Figure 2)



93. Algeria 33.77

93rd National Cyber Security Index
104th Global Cybersecurity Index
102nd ICT Development Index
100th Networked Readiness Index

Population 40.4 million
Area (km2) 2.4 million
GDP per capita ($) 15.3 thousand

Figure 2. NCSI - Algeria

Source: https://ncsi.ega.ee/country/dz/

The increasing risks still overwhelm the nation's preparation, despite the regulations on cybersecurity focusing more on the subject. According to data from the National Cybersecurity Index study, the security infrastructure is most exposed to data breaches from vital services and digital services, and the military's preparedness to carry out cyber-related operations is still only moderately high (NCSI).

Algeria has to concentrate on several issues, including the legal and legislative side, the infrastructure and mechanisms addressing cybercrimes, and the need for Algerian institutions to implement the standard ISO 27001 (ISO Standards). The most widely used standard for information security management systems (ISMS) and related requirements is ISO/IEC 27001. More than a dozen standards in the ISO/IEC 27000 family include further best practices in data protection and cyber resilience. Together, they make it possible to manage the security of assets including financial data, intellectual property, employee information, and third-party information.

To prepare a comprehensive strategy in this area and conduct digital investigations in the event of cyberattacks against national institutions (Asma, 2022), a decree related to the establishment of a national system for information systems security was passed in 2020. However, the legislative framework is still out of date, dating back to 2016 (Loi n° 16-02 du 14 Ramadan 1437) and 2018 (Law N° 18-07 relative to the Protection of Individuals in the Process). The conditions of the collection, recording, organization, conservation, adaptation or modification, extraction, consultation, use, communication by transmission, dissemination, or any other form of making available, reconciliation or interconnection, as well as locking, encrypting, erasure, or destruction of any information, whatever its source, are outlined in Law Nr. 18-07, dated on June 10, 2018. While being published in 2018, this Law's implementation is pending the real installation of the authority responsible for the protection of personal data, which has not yet been done (Hassani, 2022).

There is no particular law related to cybersecurity in Algeria. However, there are general provisions of the regulation in force applicable to different areas, which provide for the concept of the electronic privacy:

- The Criminal Code in its Articles 394bis and following protects the right of protection of the integrity of automated data processing systems;
- The Law n° 09-04 of 5 August 2009 on the specific rules relating to the prevention and the fight against breaches related to technology and communication (Law 09-04);
- The Law No. 18-04 of 10 May 2018 establishing the general rules relating to the post and electronic communications (Law 18-04);
- The Decrees related to licenses to operate public telecommunication networks;
- Decision N° 48/SP/PC/ARPT/17 dated 29 November 2017 approving the specifications defining the conditions and modalities for the establishment and operation of hosting and storage services for computerized content for user benefit in the context of cloud computing services (Decision N° 48/SP/PC/ARPT/17);
- The Decree n° 02-156 of 9 May 2002 setting the conditions for interconnection of networks and telecommunications services (Decree 02-156) (CMS, 2021).
  See Figure 3 and 4 below, which show governing bodies.

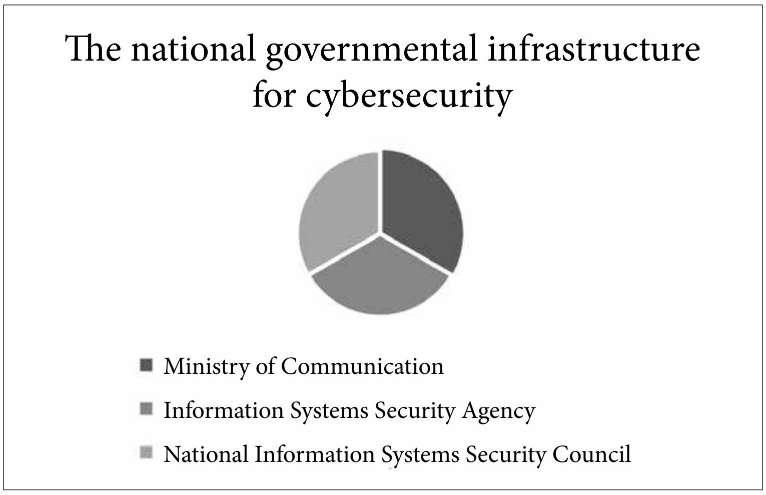


Figure 3. The national governmental infrastructure for cybersecurity

Source: https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/algeria

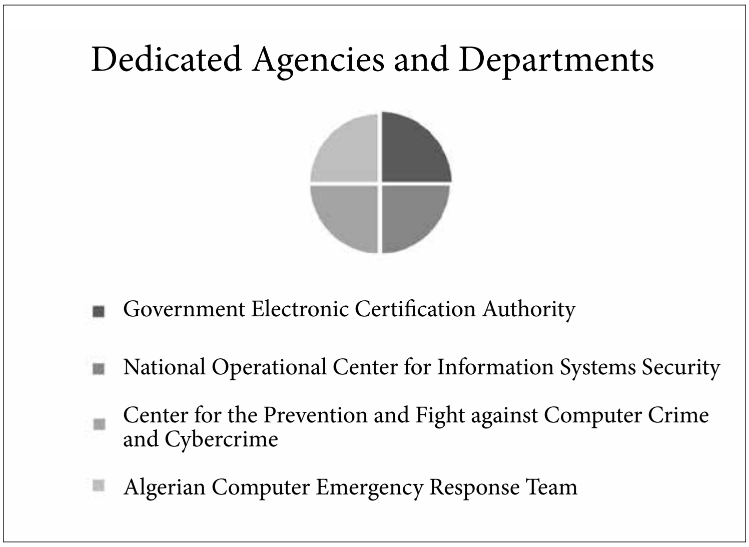


Figure 4. Dedicated Agencies and Departments

Source: https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/algeria

4. Errors, threats and attacks

The top threats according to INTERPOL’s assessment are:

- Internet scams: People are duped into disclosing personal or financial information by using phony emails or text messages that appear to be from a reliable source;
- Digital extortion, in which victims are duped into releasing pornographically explicit photos that are then used as leverage;
- Business email compromise, ransomware, and botnets are examples of cyberattacks that involve hacking into email systems to obtain information about corporate payment systems and tricking employees into transferring funds into their bank accounts.
- Ransomware locks down computer systems at hospitals and other public institutions and then demands payment to unlock the systems. (INTERPOL, 2021).

Although most criminals lack technological expertise, certain gangs are utilizing increasingly sophisticated tools to attack individuals online. During the year 2020, the Kaspersky Company has been highly effective in preventing 95,000 cyber-attacks against Algeria. This makes Algeria one of the nations most susceptible to cyber-attacks, but the corporation is making every effort to thwart them.

The nation was ranked as the least secure in the world by Kaspersky Lab in 2019, and it was still ranked fifth in 2021 (Kaspersky Security Bulletin, 2021).

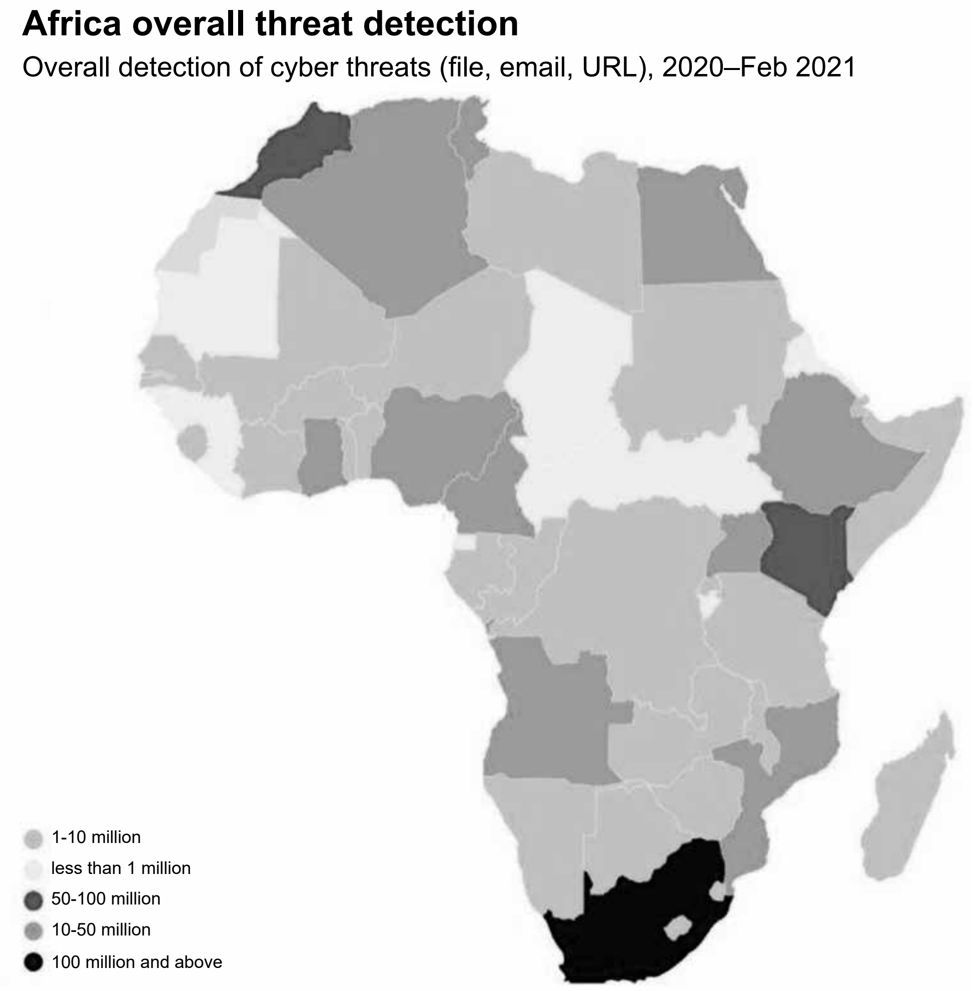

Africa overall threat detection
Overall detection of cyber threats (file, email, URL), 2020–Feb 2021
● 1-10 million
● less than 1 million
● 50-100 million
● 10-50 million
● 100 million and above

Figure 5. Interpol African Cyberthreat Assessment Report

Source: Interpol African Cyberthreat Assessment Report (pdf)

Data from the Kaspersky lab indicates that in Algeria, malware will have affected around 58.83% of ICS systems in 2022 (Kaspersky ICS CERT, 2023).

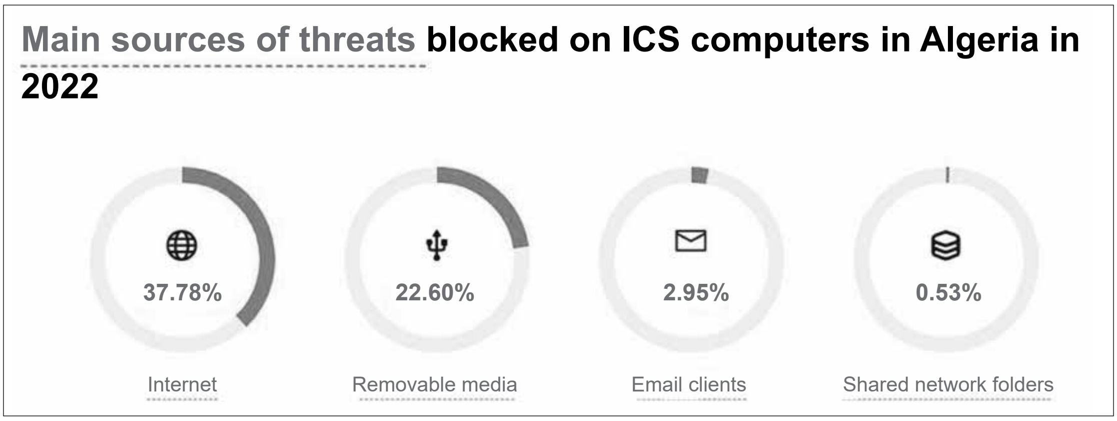


Figure 6. Kaspersky ICS CERT – Statistics

Source: https://ics-cert.kaspersky.com/statistics/

In 2020, Algeria had a substantial rise in the number of recorded crimes. Haj Said Arezki, the director of the judicial police, said that there were 258171 instances of all sorts of crimes reported for the year, including 5163 incidents of cybercrime, up from 4210 cases in 2019. These crimes include information terrorism, fraud, and damage to persons and information systems (Asma, 2022).

Although there is still a significant gap between the urgent need for an effective cyber security system and the implemented efforts, the nation is adopting security measures and modernizing its capabilities in a way that it consistently improves on indexes and positions in global databases. In the E-Government Development Index for 2018, they were ranked 130th; in 2022, they are ranked 112th (UN E- Government Knowledgebase).

In Algeria, acceptance of information security as a critical element in the development of national institutions is still conspicuously lacking. Following an investigation of several Algerian organizations involving information systems by the Algerian Association for the Security of Information Systems (AASSI) in 2015, the following conclusions were reached:

- 1% of Algerian institutions use ISO 27001 information security standard;
- 7,5 % do not have IT compliance procedures;
- 1/10 do not have activity resume plan;
- 1% have a bridge gaps management policy.

5. Conclusion

Today, Algeria is facing many challenges. The domestic political events of the recent past, as well as the continuous threat from Al Qaeda In Maghreb (AQIM) and the Islamic State (IS), as well as the long- standing foreign policy tensions, pose serious challenges to the country's leadership. In the midst of such difficulties, the question of cyber security may seem negligible at first glance, however, the wide spread of Internet technologies and the associated security risks inevitably require the introduction of international information security standards and the creation of the necessary legal background.

Equally important is the training of the appropriate professionals, the creation of organizational frameworks, and no less important is the digital hygiene education of users. These conditions are essential if the country wants to increase its internal and external security and economic competitiveness.

References

Asma, 2022. Information Security and the need to move towards the application of Standard Specifications in Algerian institutions. *Journal of Human Sciences Oum El Bouaghi University*, 9(2) https://www.asjp.cerist.dz/en/downArticle/93/9/2/190760 [Accessed 10 January 2023].

Bashir, 2022. Arab Wall: A Cyber Shadow: War between Algeria and Morocco https://arabwall.com/en/a-cyber-shadow-war- between-algeria-and-morocco/[Accessed 6 January 2023]

Besenyő, J. 2010. Western-Sahara under the Spanish empire. *AARMS*, 9(2), 195-215. [Accessed 6 January 2023]

Besenyő, J., Márton, K., & Shaffer, R. 2021. Hospital Attacks Since 9/11. An Analysis of Terrorism Targeting Healthcare Facilities and Workers. *Studies in Conflict & Terrorism*,

Besenyő, J., & Pintér, M.G. The MINURSO Police Contingent, In: János, Besenyő; Joseph, Huddleston; Yahia, H. Zoubir (eds.) Conflict and Peace in Western Sahara: The Role of the UN's Peacekeeping Mission (MINURSO), Routledge, CRC Press (2023), 368 p., pp. 182-196. (15 p) [Accessed 6 January 2023]

CMS, 2021. Data protection and cybersecurity laws in Algeria https://cms.law/en/int/expert-guides/cms-expert-guide-to-data- protection-and-cyber-security-laws/algeria [Accessed 10 January 2023].

Dessi, 2011. Cyber-Terrorism Activities Report: Electronic Jihad. *JSTOR* https://www.jstor.org/stable/resrep09473.4 [Accessed 10 January 2023].

European Commission- Global Cyber Security Index https://composite- indicators.jrc.ec.europa.eu/explorer/explorer/indices/GCI/global-cyber-security-index[Accessed 10 January 2023].

Faleg, G., & Kovalčíková, N. 2022. RISING HYBRID THREATS IN AFRICA: Challenges and implications for the EU. *JSTOR* https://www.jstor.org/stable/resrep39879 [Accessed 10 January 2023].

Hassani, 2022. OneTrust Data Guidance: Algeria - Data Protection Overview https://www.dataguidance.com/notes/algeria- data-protection-overview[Accessed 10 January 2023].

Information security management https://www.iso.org/isoiec-27001-information-security.html [Accessed 10 January 2023].

Integrated Country Strategy, 2022. Algeria https://www.state.gov/wp-content/uploads/2021/01/ICS_NEA_Algeria_Public- Release.pdf [Accessed 6 January 2023]

INTERPOL, 2021. INTERPOL report identifies top cyberthreats in Africa https://www.interpol.int/en/News-and- Events/News/2021/INTERPOL-report-identifies-top-cyberthreats-in-Africa [Accessed 10 January 2023].

ISO Standards. ISO/IEC 27001 and related standards: Information security management https://www.iso.org/isoiec-27001- information-security.html [Accessed 10 January 2023].

Kaspersky ICS CERT, 2023. Statistics https://ics-cert.kaspersky.com/statistics/ [Accessed 10 January 2023].

Kaspersky Security Bulletin, 2021. Statistics https://go.kaspersky.com/rs/802-IJN-240/images/KSB_statistics_2021_eng.pdf [Accessed 10 January 2023].

Kasraoiu, 2022. Morocco World News: Algerian Hacker Attacks Website of Science University in Fez, Morocco https://www.moroccoworldnews.com/2022/08/350651/algerian-hacker-attacks-website-of-science-university-in-fez-morocco [Accessed 6 January 2023]

Kovács, A. M. 2022. Ransomware: a comprehensive study of the exponentially increasing cybersecurity threat. *Insights into Regional Development,* 4(2), 96-104. https://doi.org/10.9770/IRD.2022.4.2(8)

KPMG, 2022. Africa Cyber Security Outlook https://assets.kpmg/content/dam/kpmg/za/pdf/2022/KPMG%20Africa%20Cyber%20Security%20Outlook%202022_Report_ Sep%2012_Low%20Quality.pdf [Accessed 10 January 2023].

League of Arab States General Secretariat, 2012. Arab Convention on Combating Information Technology Offences https://nsarchive.gwu.edu/document/18573-national-security-archive-arab-convention [Accessed 6 January 2023]

MacGibbon. 2015. Assessing Cyber Security: A Meta-Analysis of Threats, Trends, and Responses
to Cyber Attacks. *JSTOR*, 57-72 (17 pages) https://www.jstor.org/stable/resrep12567.7 [Accessed 2 January 2023].

Mitchell, 2022. Investment Monitor: Africa faces huge cybercrime threat as the pace of digitalisation increases https://www.investmentmonitor.ai/features/africa-cyber-crime-threat-digitalisation/ [Accessed 6 January 2023] NCSI. (https://ncsi.ega.ee/country/dz/) [Accessed 10 January 2023].

NCSI. https://ncsi.ega.ee/ncsi-index/?order=-rank[Accessed 10 January 2023].

Ndemo, 2021. New Conditions and Constellations in Cyber: Digital Transformation and Cyberstability: Effects on Economic Development in Africa. https://www.jstor.org/stable/resrep38794.13 [Accessed 3 January 2023].

Project CyberSouth, 2017. Cooperation on cybercrime in the Southern Neighbourhood https://rm.coe.int/cybersouth- summary-of-the-project/1680731824 [Accessed 6 January 2023]

Ramluckan & Niekerk, 2020. Journal of Information Warfare - Cybersecurity and Information Warfare Research in South Africa: Challenges and Proposed Solutions. https://www.jstor.org/stable/27033610 [Accessed 2 January 2023].

Turianski, 2020. Balancing Cyber Security and Internet Freedom in Africa. *JSTOR* https://www.jstor.org/stable/resrep25912 [Accessed 2 January 2023]

U.S. Attorney's Office, 2013. Algerian National Extradited from Thailand to Face Federal Cyber Crime Charges in Atlanta for SpyEye Virus https://archives.fbi.gov/archives/atlanta/press-releases/2013/algerian-national-extradited-from-thailand-to-face-federal-cyber-crime-charges-in-atlanta-for-spyeye-virus [Accessed 10 January 2023].

UN E-Government Knowledgebase. Algeria https://publicadministration.un.org/egovkb/en-us/Data/Country- Information/id/3-Algeria/dataYear/2022 [Accessed 10 January 2023].

WorldData.info. Telecommunication in Algeria https://www.worlddata.info/africa/algeria/telecommunication.php[Accessed 10 January 2023].

Zoltán SIPOS
ORCID ID: https://orcid.org/0000-0001-7017-571X