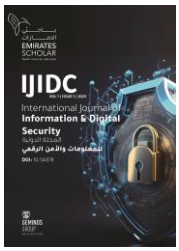

International Journal of Information & Digital Security
Vol 2 Issue 1 (2024)
Pages (29 –39)

Available at www.emiratesscholar.com

Morocco's cybersecurity strategy between challenges and aspirations

Driss Abbadi
drissali@hotmail.fr
Department of Legal, Political and Economic Research, University of Sidi Mohamed Ben Abdel Allah, Fez, Morocco.

ARTICLE INFO

Published on 30th of December 2024
Doi: 10.54878/acgprq10

KEYWORDS

Strategy, Cybersecurity, Morocco, Cyber Challenges, Cyber Aspirations.

HOW TO CITE

Morocco's cybersecurity strategy between challenges and aspirations. (2024). *International Journal of Information & Digital Security*, *2*(1), 29-39.

ABSTRACT

The threats and challenges associated with the cyberspace have increased, and no country is excluded from its economic, social and cultural activities on the Internet, and Morocco has also not been spared some digital machinations to harm its cyberspace. For this reason, the contours of its cyber strategy have been prominent since 2012 to counter the risks coming from the virtual world. This strategy focused on the establishment of national institutions specialized in cyber securitization, benefiting from international and regional partnerships, and did not neglect the issuance of laws and the signing of regulatory agreements. But this strategy has run into some challenges resulting from legal loopholes and treaty reservations. Despite these challenges, Morocco has registered a strong desire to develop its capabilities and strengthen its position in the global cybersecurity index, by benefiting from international experiences and foreign companies specialized in cyber issues, and by including digital education in its university institutions.

1. Introduction

The concerns of most countries have intensified as they transitioned from an industrial paradigm to a post-industrial orientation linked to information and knowledge systems (Barney, 2015), primarily based on the digital realm, which has come to occupy a crucial position in the modern era. It is undeniable that the lives of nations, companies, and citizens have been inundated by new information and communication technologies, and the world has become increasingly computerized and interconnected, yet not immune to digital risks (BELGOURCH et al., 2020, p. 221). This contemporary digital dominance has shattered traditional geographical boundaries, disrupted closed cultures, and reshaped communities and social identities. These accumulations have contributed to the creation of what is known as the "Network Society" (Swellmi, 2021, pp. 133-134).

For this reason, there is global concern that cyberspace may become the target of future attacks (Grange, 2014, p. 4). This concern did not emerge by chance but became evident in the late 1990s, when the first cyberattacks occurred during the Yugoslav conflict, followed by attacks targeting Estonia and Georgia in 2007, and then the spread of the Stuxnet virus, which targeted Iran in 2010 (Rabussier, 2018-2019, p. 15). Since then, most countries, including Morocco, have paid attention to their cybersecurity and have developed strategies to confront the risks present in this domain.

2. Conceptual Framework

The term "governor" is metaphorically used (Al-Quraity, 2021, p. 11). Referring to the "Al-Mawrid" dictionary, cyberspace is defined as the science of control, with its root in "cybernetics," a term that aligns with the concept of cyberattacks, which involve controlling and regulating things remotely. Meanwhile, the U.S. Military Terminology Dictionary defines cyberattacks as actions intended to seize or damage other electronic programs. Additionally, the Information Security Terminology Dictionary defines cyberattacks as: "An attack through cyberspace aimed at controlling electronically protected websites or infrastructure to disrupt, destroy, or damage them" (Al-Fatlawi, 2018, pp. 11-12).

In the Arabic language, we note the absence of a corresponding term for "cyber," as it was retained in its original form, first used by American mathematician Norbert Wiener in the late 1940s (Al-Fatlawi, 2018, pp. 11-12). Wiener is considered the founding father of cybernetics through his famous work Cybernetics or Control and Communication in the Animal and the Machine. In his book, he referred to cybernetics as the science of control and communication in animals, machines, and humans. After World War II, the term "machine" was replaced by "computer" (Al-Quraity, 2021, pp. 11-12).

3. Significance of the Study

The significance of this study lies in its focus on a pivotal topic at the scientific level, falling within the realm of security and strategic studies. This topic has gained considerable importance, especially in recent times, as it aims to examine the strategy adopted by Morocco to secure its cyberspace, while highlighting the challenges it faces and the aspirations it seeks to achieve in this domain.

4. Research Problem

Morocco's cybersecurity strategy began to take shape in 2012 when its Strategic Committee for the Security of Information Systems (CSSSI) adopted the first National Cybersecurity Strategy. This strategy focused on four main pillars: risk assessment, protection of the information systems of government agencies, public institutions, and critical infrastructure, strengthening the foundations of information systems security (legal framework, awareness, training, and research and development), and promoting national and international cooperation (Hathaway & Spidalieri, 2018, p. 7). However, despite this strategy aimed at mitigating cyber risks, Moroccan official institutions still occasionally report cyberattacks targeting the country.

Given this context, the core problem of this article revolves around Morocco's strategy for managing its cyberspace, highlighting the challenges it faces and the aspirations it seeks to achieve in this field. This problem needs to be broken down to better understand its dimensions, which can be achieved by addressing the following key questions:

-What is Morocco's strategy for addressing cyber threats?

-What challenges does Morocco face in securing its cyberspace?

-What are Morocco's aspirations for strengthening its cybersecurity?

5. Study Methodology

The study adopted the systemic approach to explore the inputs embedded in Morocco's cybersecurity strategy, highlight the challenges it faces, and clarify its feedback, which is reflected in the aspirations it seeks to achieve. Additionally, the study employed the descriptive-analytical method to describe and analyze the phenomenon under investigation.

6. Research Outline

-**First Section:** Morocco's Cybersecurity Strategy

-**Second Section**: The Challenges of Moroccan Cybersecurity Between Threats and

Aspirations

First Section: Morocco's Cybersecurity Strategy

It has become essential for countries worldwide to adopt cybersecurity strategies to confront the risks emerging from the virtual world. Morocco has also recognized this need, adopting its own strategy to address this challenge, which is based on establishing national institutions, forging international and regional partnerships, and enacting regulatory laws and agreements.

1. Morocco's Institutions and Partnerships in the Cybersecurity Domain

Since 2012, Morocco has pursued a unique strategy to address cybersecurity challenges. This strategy has focused on creating national institutions, benefiting from international experiences, and establishing international and regional cooperation partnerships.

11. National Institutions and International Experiences in Cybersecurity

Morocco has established several regulatory institutions to implement its cybersecurity strategy. These include the Strategic Committee for the Security of Information Systems (CSSSI), founded in 2011, and the General Directorate of Information Systems Security (DGSSI), created in 2011 under the National Defense Administration (ADN) and overseen by the CSSSI. The DGSSI is responsible for developing and implementing the national cybersecurity strategy. Another institution is the National Commission for the Protection of Personal Data (CNDP), tasked with safeguarding personal data. The Moroccan Computer Emergency Response Team (ma-CERT) was established under the direction of the ADN to combat cyber threats. Additionally, regional digital forensic labs for tracking and analyzing cybercrimes have been set up under the General Directorate of National Security (DGSN). Furthermore, the National Telecommunications Regulatory Agency (ANRT) has been elevated to a governmental authority closely associated with telecom operators and internet service providers (ISPs). Morocco has also begun updating and strengthening its legal and regulatory framework to address cybercrimes and protect data (Hathaway & Spidalieri, 2018, p. 7).

Morocco has also sought to benefit from international experiences in cybersecurity by hosting events related to cybersecurity in collaboration with the World Bank, the International Telecommunication Union, and NATO's Science for Peace and Security Programme (Hathaway & Spidalieri, 2018, pp. 22-23). It has participated in several dialogues with European countries, the United States, and Gulf Cooperation Council (GCC) members on security issues, counterterrorism operations, and the use of cyberspace by terrorists and other criminal groups

12. Morocco's Cybersecurity Partnerships

Morocco seeks to establish international and regional partnerships to create a cooperative framework for tightening the noose on cyber attackers and fostering regional and international digital trust. Most countries worldwide, including Morocco, have taken steps to enhance their cooperation against cybercrime at the international level alongside national efforts (Jouy, 2022, pp. 2-12). For Morocco, partnerships have been established with the European Union and NATO. With respect to the European Union, there are several constants and variables that determine Morocco's security position in its relations with the EU, including its geographical proximity to Europe and its historical legacy, as well as its political and strategic attributes that have made it a key interlocutor for many European powers in the security domain (Hilali, 2022). Morocco’s Mediterranean identity and its geographical proximity to Europe necessitate its engagement with EU countries in multidimensional partnerships related to cybersecurity and other fields. Morocco is considered a significant factor in the European security equation, with its strategic location qualifying it to play the role of "guardian" of European borders against security threats and maintaining Mediterranean security (Hilali, 2022).

Regarding NATO, the institutionalization of relations between Morocco and NATO began in 1994, when

NATO was concerned about the lack of security south of its borders. In 2004, during the Istanbul Summit, it was proposed to improve dialogue by increasing the areas of cooperation and meetings between the two parties. Morocco is often a candidate for participating in some NATO missions in Europe (Elniya, 2020). The Alliance's desire to establish strong relations with Morocco is evidenced by its organization of seminars and visits to Moroccan military facilities by NATO authorities, and the signing of agreements to facilitate the exchange of confidential information and participation in peace and security programs (Roldan Barbero, 2018). While cyber threats to the Alliance's security are complex, destructive, coercive by nature, and increasingly frequent, NATO continues to adapt to the evolving landscape of these threats. The organization and its allies (with Morocco being one as a Major Non-NATO Ally, MNNA) have relied on strong and resilient cyber defense assets since the 2014 NATO Summit in Wales to accomplish the Alliance's core missions of collective defense, crisis management, and cooperative security. The 2014 policy established that cybersecurity is part of NATO's core mission of collective defense, endorsed that international law applies to cyberspace, and enhanced NATO and its allies' capabilities. At the Warsaw Summit in 2016, allies reaffirmed NATO's defensive mandate and acknowledged that cyberspace represents an operational environment requiring NATO to bolster its defenses similarly to its defense in air, land, and sea. In 2021, at the NATO Summit in Brussels, allies adopted a new comprehensive cybersecurity policy, which contributes to NATO's three core missions (collective defense, crisis management, and cooperative security) and its overall stance on deterrence and defense (North Atlantic Treaty Organization, 2023).

It is evident that Europe, represented by the European Union and NATO, has a strong geopolitical relationship with Morocco, considering it a strong strategic ally outside of NATO. As the European Union and NATO continue to develop their cybersecurity frameworks, Morocco benefits from this partnership with them.

2. Laws and Agreements Governing Moroccan Cybersecurity

The study aimed to outline the main laws and agreements regulating the digital domain in Morocco to assess the extent to which Morocco is working to achieve its cybersecurity goals.

21. Domestic Laws Governing Moroccan Cybersecurity

The Moroccan legislator had to enrich the Penal Code with provisions that might apply to crimes occurring in its cyberspace. This led to the emergence of a set of laws in 2003, which complemented the Penal Code regarding automated data processing systems (Elazzouzi, 2010, p. 113).

Morocco, therefore, established a range of national cybersecurity measures due to its exposure to cyber attacks, like all other countries (Elazzouzi, 2010, p. 113). It also aimed to improve the legal and regulatory framework to better protect society from cyber crimes and align with partner countries (Hathaway & Spidalieri, 2018, p. 16). Among the measures Morocco has initiated, we note the establishment in 2011 of entities responsible for creating a comprehensive legal and technical framework to ensure the security of information systems (Elazzouzi, 2010, p. 113). In 2016, a decree on the protection of the sensitivity of information systems and infrastructure was issued, imposing strict data protection requirements, including reducing cross-border data flow and setting data storage requirements (Speek & Barqia, 2021, p. 15). Additionally, Moroccan legislation has introduced a legal arsenal; in 2013, Law No. 24.96 was amended by Law No. 93.12 (Law No. 93.12, 2013, p. 4874), which transferred and reallocated several powers from the National Telecommunications Regulatory Agency to the Ministry Delegate to the Head of Government responsible for National Defense Administration (Antar, 2019, p. 22). To enhance the legal framework for cybersecurity, the Moroccan government decided on May 15, 2014, through Decree No. 881-13-02, to have the National Defense Administration (ADN), specifically the General Directorate for Information Systems Security, oversee all activities related to encryption (Sbihi, 2021). In 2016, the General Directorate for Information Systems Security (DGSSI) issued a decree defining the protection system for sensitive information systems in critical infrastructure. This text was enacted through a decree by the Head of Government in 2018 (Sbihi, 2021). Additionally, we must not overlook Law No. 05.20 (Law No. 05.20, 2020, p. 4160), which aims to provide a legal framework including minimum rules and security measures to ensure the reliability and resilience of information systems. It also aims to enhance digital trust, digitize the economy, ensure the continuity of economic and societal activities in Morocco, and develop a cybersecurity ecosystem in the country

(Speek & Barqia, 2021, p. 15). Thus, Morocco's cyber security law has been strengthened and updated through the implementation of Law No. 20-05 (Sbihi, 2021).

22. International and Regional Agreements Regulating Moroccan Cybersecurity

The study in this section focused on the international and regional agreements that Morocco has ratified to achieve its cybersecurity. Regarding international agreements regulating Moroccan cybersecurity, these agreements take various forms, such as extradition of criminals, judicial assistance, mutual recognition of res judicata, and informal coordination between relevant military and security agencies (Jabbour, 2016, p. 102). This is the method adopted between states concerning traditional issues. However, regarding issues related to the cyber world, despite significant efforts to strengthen national cyber capabilities, no international consensus has been reached so far on the application of the "Law of Armed Conflict (LOAC)," sometimes referred to as LOW or the "Law of War," to cyberattacks. These attacks are often considered a form of "irregular attacks" (Jabbour, 2016, p. 103). Some argue that the provisions of international humanitarian law can be applied to cyberattacks, due to several reasons, including the flexible nature of its texts and principles, with perhaps the most important being the "Martens Clause," which is considered the safety valve and the optimal solution for subjecting cyberattacks to the provisions of international humanitarian law (Al-Samarrai, 2023, pp. 140-141). Despite these efforts in public international law to contain and deter the risk of cyberattacks, there are real challenges that hinder most international initiatives aimed at curbing the cyber threat.

At the regional level, specifically in the Arab region, an Arab Convention was established on December 21, 2010, to combat information technology crimes. Twenty-one (21) countries, including Morocco, signed the convention, but only seven countries have ratified it (Al-Bidri, 2021, pp. 105-106). According to the provisions of Article 1, the aim of this convention is to enhance cooperation between member states in combating information technology crimes, given the threat they pose to the security, interests, societies, and individuals of these states (Al-Razi, 2019, p. 31). Additionally, ESCWA, within the framework of the "Coordination of Cyber Legislation to Stimulate a Knowledge Society in the Arab Region" project, implemented between 2009-2012, developed the "ESCWA Guidelines for Cyber Legislation," which serve as legislative models for countries in the region. These guidelines cover not only cybercrime but also electronic communications, freedom of expression, electronic signatures, e-transactions, e-commerce, consumer protection, the processing of personal data, and intellectual property rights in the information and cyber domain (Al-Bidri, 2021, pp. 105-106).

At the African level, the "Malabo Convention" on cybersecurity and the protection of personal data was adopted by the African Union countries in 2014, and it has been ratified by several African countries, including Morocco. Morocco prepared Law No. 52.21, approving this convention adopted in Malabo, Equatorial Guinea (Al-Bidri, 2021, pp. 105-106). This convention was concluded in several stages, from the launch of the project and the drafting of the initial convention to its adoption and the opening for signatures (Lokal, 2021, pp. 657-661)

Based on what was discussed in the first section, it is clear that Morocco has adopted a well-defined strategy in the cyber field. However, this strategy continues to face real challenges that hinder its normal progress. These challenges push the official authorities in Morocco to seek effective ways to counter them, which is what the study explored in its second section by delving into these challenges and examining future aspirations.

Second section: The Challenges of Moroccan Cybersecurity Between Threats and Aspirations

The increasing threats and challenges related to cyberspace have not spared any country that relies on the internet for its economic, social, and cultural activities (Al-Bidri, 2021, pp. 108-109). Morocco, too, has not been immune to various digital schemes aimed at harming its cyberspace. For this reason, it becomes evident that Morocco is not fortified against cyber threats and has faced them multiple times (Mouhir & Mokhtar, 2023). Based on the above, this study aims to highlight the challenges facing Moroccan cybersecurity while also outlining the aspirations it seeks to achieve.

1. The Challenges Facing Moroccan Cybersecurity

Cyberspace has transformed into a primary battleground for both traditional and non-traditional conflicts. In this space, enemies include states and non-state entities, ranging from amateur hackers to professional cybercriminals. These actors target

various sectors such as industry, academia, government, and the military across air, land, sea, and space domains. One of the prominent features of the global political system is the increasing number and significance of non-state actors, which poses a real challenge to traditional international relations theories that assume states are the primary units of the international system (DeLuca, 2013, p. 279). This introduction leads us to explore the challenges hindering the advancement of Moroccan cybersecurity, whether they stem from the difficulty of enforcing cyberspace regulations or challenges related to the implementation of international and regional agreements.

11. Legal Gaps: Despite the efforts of countries worldwide, including Morocco, to implement laws regulating their cyberspace, these efforts seem weak compared to the challenges faced and the obstacles that hinder their application. These obstacles include the limitations of domestic laws governing Moroccan cybersecurity and challenges related to the enforcement of international laws protecting cybersecurity. As for the limitations of domestic laws, Morocco has indeed made legal and technical progress in combating cybercrime. However, the regulatory framework remains limited to vital organizations and largely ignores the private sector (Pollack et al., 2021, p. 20). Moreover, cybercrimes continue to evolve in ways that cannot be punished in the same manner as traditional crimes under the conventional criminal code. While there are numerous legal texts criminalizing computer crimes, they are often circumvented (Missaoui & Elhila, 2021). Although Moroccan criminal law is based on a set of fundamental principles, such as the principle of legality and strict interpretation of criminal law, these core principles are undermined by the cybercrime scourge (Missaoui & Elhila, 2021). Cybercrime represents a significant challenge for Moroccan security, as it evolves in tandem with information and communication technologies (ICT), while the Moroccan legal framework takes considerable time to be enacted. This highlights a contradiction on two levels: first, between the rapid development of ICT and cybercrimes, and second, the slow implementation of a legal framework aimed at combating cybercrime. For example, when it comes to the criminal code, one of the major challenges limiting its role in combating cybercrime is the difficulty in justifying certain crimes, proving intent, identifying perpetrators, and prosecuting crimes committed online (Roumate, 2023, p. 4).

Similarly, the obstacles to enforcing international laws protecting Moroccan cybersecurity are no less significant than the aforementioned challenges. To clarify these obstacles that prevent the application of international laws in Morocco’s cyberspace, we can refer to the general obstacles hindering the enforcement of international laws in the cyber field. The United Nations Charter addressed the legal limitations on the use of force in international law and relations between states. Article 2, Paragraph 4 of the UN Charter states that: "All members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations." Here, force is associated with classical, hard power. However, with unprecedented technological advancements, a new form of power has emerged—cyber power—along with uncertainty about how to handle it (Kareem, 2021, pp. 321-322). It is logical for international law governing wars to evolve in parallel with the development of cyber warfare, yet with the increasing frequency of cyberattacks, a legal dilemma has arisen regarding the classification of these attacks (Abdelwahid, 2021, p. 48). This new phenomenon, "cyber warfare," has posed a real challenge in the field of international law concerning the legal framework for this type of attack. Specifically, the dilemma of identifying the actor (the aggressor) has emerged, which contrasts with traditional methods of warfare (International Committee of the Red Cross, 2019, p. 5). Furthermore, even when examining the legal systems of many countries dealing with cybercrime, it becomes clear that there is no common international agreement on which types of internet misuse should be criminalized. What is permissible under one system may be criminalized in another. Another challenge is the issue of jurisdiction: a crime may be committed within the territory of one state by a foreigner, and in such cases, the crime falls under the criminal jurisdiction of the first state based on the principle of territoriality, but it may also fall under the jurisdiction of the second state based on personal jurisdiction. Additionally, the crime may threaten the security and safety of a third state, thus falling under its jurisdiction based on the principle of universality (Al-Touni, 2023, pp. 161-164).

12. Reservations on Regional and International Agreements Governing Moroccan Cybersecurity

Most countries, including Morocco, attempt to mitigate cyber threats through regional and

international agreements, but the implementation of these agreements faces certain reservations.

Regarding the reservations recorded on regional agreements governing Moroccan cybersecurity, Africa, in general, and Morocco, in particular, face an increasing array of cyber threats, including espionage, sabotage of critical infrastructure, anti-innovation, and organized crime. Many African countries still need to develop national strategies to secure their cyberspace. Even those African countries with cybersecurity strategies often fail to achieve meaningful impact, as their plans lack foundational elements and do not adapt to the changing threat landscape (Ajijola & Allen, 2022). Additionally, the continent suffers from a stark shortage of cyber defense. This is exemplified by the incident where China spied on the African Union headquarters from January 2012 to January 2017. While there is regional cooperation in cyber defense, it remains ineffective, as evidenced by the "Malabo Convention." Strangely, the Malabo Convention was adopted in 2014 but has not yet entered into force, reflecting that many African countries still do not consider cybersecurity a vital issue, exacerbating the problem (Loukal, 2021, p. 667).

As for the reservations on international agreements governing cybersecurity, cyberattacks have spread rapidly among countries, posing a significant challenge even to international treaties and agreements (Bories, 2014). This challenge is evident in the limitations of these international agreements to provide cybersecurity for countries globally, and specifically for Morocco, as revealed by Edward Snowden's 2013 disclosures about the NSA's mass internet surveillance program. These revelations showed that the techniques and agreements of any country remain vulnerable to the dominance of major powers in information and communication technology (ICT). Snowden's disclosures led to a loss of trust in these technologies and agreements, and in U.S. cyber activities. The Snowden case sparked outrage and reflection among nations about how to protect their cyber sovereignty. National sovereignty was violated through such interventions and massive espionage campaigns (Mlih, 2021, p. 228).

In this context, it is worth noting that despite the agreements Morocco has signed with various countries in the field of cybersecurity, it still experiences security gaps regarding the protection of its websites. These agreements have resulted in the establishment of centers focused only on alerting and managing information incidents, rather than preemptively preventing attacks. For example, the agreement Morocco signed with South Korea led to the creation of the Moroccan Center for Incident Response and Management by the Ministry of Industry, Trade, and Modern Technologies, in cooperation with the Korean International Cooperation Agency (Antar, 2019, pp. 22-23).

These agreements also suffer from other limitations. The Budapest Convention, for instance, has two major constraints: the first is geographic, as only 49 countries have ratified this text, and the second is related to the proliferation of dark web and deep web markets, where forums take into account the specificities of malicious computing tools and related services, making it particularly difficult to suppress the misuse of devices (Gery, 2018, pp. 43-54).

Furthermore, international cooperation in cyberspace is limited to combating cybercrime and does not extend to addressing threats posed by states against other states. This is because major powers that employ offensive cyber tactics to achieve their objectives are not interested in regulating such attacks. Additionally, there are differing views on how to regulate cyberspace (Antar, 2019, pp. 22-23).

The issue of mistrust between major cyber powers, such as the United States and China, has also significantly delayed the signing of several international agreements (Al-Fatlawi, 2018, p. 105). Even when efforts are made to combat these delays, there are obstacles that make such cooperation difficult to achieve. These obstacles can be summarized as follows:

1. The absence of a universally agreed-upon model regarding criminal activity due to differences in legal systems around the world and their inability to agree on a specific definition of the criminal activity to be prosecuted. This is largely due to the legislative shortcomings in many countries and their inability to keep pace with the rapid advancement in information technology and, consequently, cybercrime (Qataf, 2022, p. 21).

2. The lack of bilateral or multilateral treaties between states that would allow for fruitful cooperation in the cyber domain, and even when they do exist, they are often insufficient to provide the necessary protection (Qataf, 2022, p. 21).

Despite these legal gaps and the reservations recorded on regional and international agreements governing cyberspace in Morocco, the country looks to fortify its cyberspace by relying on international experiences and foreign companies specialized in cybersecurity, as well as encouraging its universities to focus on cybersecurity studies.

2. Morocco's Cybersecurity Aspirations

Despite the aforementioned challenges, Morocco demonstrates a strong desire to develop its cybersecurity. This desire is confirmed by its seventh-place ranking in the Arab Cybersecurity Index, 50th place in the Global Cybersecurity Index, achieving a 100% score in the ICT Development Index, and ranking 31st out of 160 countries in the 2022 Network Readiness Index, along with notable performances in other assessments (Indice de Cybersécurité, 2022).

To further illustrate Morocco's ambition to enhance its cybersecurity, the study highlights Morocco's benefit from international experiences and foreign companies specializing in the cyber domain, and addresses the role of Moroccan education in fostering digital trust.

21. International Experiences and Foreign Companies Specializing in Securing Morocco's Cyber Space

Morocco signed an agreement with South Korea that led to the establishment of the Moroccan Center for Incident Response and Management "maCert" in 2011, created by the Ministry of Industry, Trade, and New Technologies and the Korea International Cooperation Agency (Antar, 2019, pp. 22-23). Additionally, a memorandum of understanding was signed with India outlining a general framework for cooperation in cybersecurity between Morocco's National Defense Administration and its Indian counterpart. This cooperation includes expertise exchange in cybersecurity technologies, best practices, and training, and resulted from the visit of Morocco's Deputy Minister to the Indian Prime Minister, responsible for national defense, from September 24 to 27, 2018 (Al-Bidri, 2021, pp. 112-113).

Moreover, in addition to national players, Morocco's cybersecurity sector has opened up to foreign companies that have invested in Moroccan cyber defense. For example, in 2013, the General Directorate for Economic and Social Crimes and "ANSSI" signed a cooperation agreement, and Moroccan representatives in 2018 ratified the Budapest Convention on Cybercrime. That same year, the kingdom joined the "Cyber South" cooperation project with the European Union and other Mediterranean countries (Mouhir & Mokhtar, 2023). Additionally, there are American companies like Symantec, Fortinet, and Palo Alto Networks; European actors like Bitdefender and Kaspersky; and French companies like Orange-Morocco, Orange-Cyberdefense, Thales, Devoteam, and Atos. There are also mid-sized actors in the Moroccan market, such as "6cure," a French publisher of anti-DDoS solutions, which has enabled Moroccan companies and operators to establish trusted digital spaces, and "Systancia," a French expert in virtualization, cybersecurity, and digital trust. Furthermore, the Cypriot company "Secmentis," which serves Morocco from its headquarters in Limassol, specializes in penetration testing, threat intelligence, and proactive defense of IT infrastructure (Mouhir & Mokhtar, 2023).

22. Moroccan Education and the Promotion of Digital Trust

IT tools have become essential to workplace quality of life. In this context, on November 15, 2023, the Ministry of Digital Transformation and the Ministry of Higher Education signed a partnership to implement a program to boost digital graduates in Moroccan universities. Morocco offers an educational environment across all sectors, including digitization. Moroccan universities aim to cultivate a generation well-versed in digital developments. The Minister of Finance, responsible for the budget, Fouzi Lekjaa, together with Prime Minister Aziz Akhannouch, participated in the signing ceremony for an agreement aimed at implementing a plan to increase the number of students and graduates in the digital field within public universities by 2027. As part of this partnership, Minister of Digital Transformation and Administrative Reform, Ghita Mezzour, mentioned that "the new training programs will include data analysis, big data, IT security, digital technologies, and cybersecurity, in twelve university institutions across different regions of the kingdom." According to the Ministry of Digital Transition and Administrative Reform, this agreement aims to design and implement new digital university training programs across Moroccan public universities to meet labor market needs and investors' expectations, and to increase the number of graduates, currently 8,000 annually across various disciplines (El Haddad, 2023).

Some Moroccan scientific and technical schools and universities have started integrating computer-related courses into their science programs and other curricula related to cybersecurity, to meet the growing demand for skilled workers at the national level (Hathaway & Spidalieri, 2018, pp. 20-21).

The government has also recognized the necessity of upgrading workforce skills and training IT managers in cybersecurity. Therefore, the National Telecommunications Regulatory Agency (ANRT) began funding an executive master's program in cybersecurity at the National Institute of Posts and Telecommunications (INPT) for public sector employees, supported by the General Directorate of Information Security (DGSSI) and the Office for Vocational Training and Labor Promotion (OFPPT). A training academy has been established to enhance mid-career professional skill development in IT and information security. A national cybersecurity framework (sector-specific) was also approved for certifying and accrediting professionals in public and national agencies. This project, called the Professional Master's Program for Training and Certification of Professionals in the Public Sector, aims to further this goal (Hathaway & Spidalieri, 2018, pp. 20-21).

Additionally, in February 2016, the Moroccan Ministry of Industry, Trade, Investment, and Digital Economy, in collaboration with Moroccan universities and public and private institutions, launched the "National Cybercrime Prevention Campaign." Led by the Moroccan Center for Research and Innovation in Polytechnic (CMRPI) in Rabat, this annual campaign aims to raise private sector awareness about cybercrime and promote security in technology usage in society by integrating international best practices (Hathaway & Spidalieri, 2018, pp. 20-21).

Regarding private Moroccan universities, such as EUROMED, cybersecurity has become a significant influence in academic research and business. The launch of cybersecurity training at UEMF aligns with the Ministry of Higher Education's goal to develop university training in Morocco, encourage scientific research in this field, and engage with industry leaders, giving Moroccan universities access to technological tools and developments in cybersecurity (Ecole d'Ingénierie Digitale et d'Intelligence Artificielle, 2023). Cybersecurity training at this university aims to train cybersecurity engineers through modules, practical work, and internships in companies, allowing them to gain experience in implementing security measures for information systems, identifying vulnerabilities, executing counterattacks, and raising user awareness. The training program is based on methodologies for designing, organizing, and auditing information system security, cryptography, blockchain, secure systems, network architecture, security deployment, supervision, and auditing. Graduates will be capable of understanding, modeling, designing, managing, maintaining, or improving secure embedded systems, integrated systems, secure communication objects, or secure sensor/actuator networks (Ecole d'Ingénierie Digitale et d'Intelligence Artificielle, 2023).

Conclusion

Since 2012, Morocco has been striving to adopt a national strategy to address cybersecurity challenges. This strategy has been built on creating national institutions, learning from international experiences in cybersecurity, and forming international and regional cooperation agreements. It also includes legal measures and agreements regulating Morocco's digital space. However, the increasing threats and challenges related to cybersecurity have not spared any country that relies on the internet for economic, social, and cultural activities. Morocco, too, has suffered from cybersecurity incidents, whether due to difficulties in enforcing laws governing cyberspace or issues related to the limitations of international and regional agreements.

Despite these shortcomings, Morocco shows a strong desire to improve its cybersecurity. This is evident in its upward rankings in global cybersecurity indices, benefiting from international experiences and specialized foreign companies, and efforts by its universities to promote digital trust.

However, the question remains: When will Morocco be able to develop its own mechanisms to secure its cyberspace without relying on the tools of dominant global players in the cybersecurity field? This is a topic for another discussion.

Sources and References

In Arabic

Books

1. Al-Fatlawi, A. A. N. (2018). Cyber Attacks: A Legal and Analytical Study on the Challenges of Contemporary Regulation. Beirut: Zain Legal and Literary Publications.

2. Al-Quraiti, D. H. (2021). Cybersecurity and Information Security Protection. Alexandria: University Thought House.

3. Al-Samarrai, M. (2023). The Role of International Law in Combating Cyber Attacks. Baghdad: Memory Publishing and Distribution.

4. Al-Tuni, M. A. M. (2023). Cyber Attack Mitigation Strategies. Alexandria: University Thought House.

5. Barney, D. (2015). The Networked Society (translated by Anwar Al-Jammawi). Translation Series. Beirut: Arab Center for Research and Policy Studies.

6. Jabbour, M. A. (2016). Cybersecurity: The Concern of Our Era. Arab Center for Legal and Judicial Research.

7. Swailmi, M. (2021). In Digital Islam: How Muslims Moved to Cyberspace. Tunis: Tunisian House of Books.

Theses and Dissertations

8. Abdul Wahid, S. H. (2020-2021). Cyber Wars: A Study of Their Concept, Characteristics, and Means of Confrontation (Master's Thesis, Middle East University, Faculty of Arts and Sciences, Jordan).

Articles

9. Al-Bidri, A. W. (2021). Cybersecurity Strategy: A Case Study of Morocco. Journal of Strategic and Military Studies, Arab Democratic Center for Strategic, Political, and Economic Studies, retrieved from: bit.ly/4cY1uU0

10. Al-Razi, S. M. A. (2019). Cybercrime and the Integration of National, Regional, and International Texts. International Law and Business Journal, Series of Publications and Works of Hassan II University, (23).

11. Pollack, B., Burhan, R., et al. (2021). Great Expectations: Defining the Cybersecurity Agenda Across the Mediterranean. Journal of the European Institute of the Mediterranean, (22).

12. Speck, B., & Barqia, A. (2021). Cybersecurity... The New Generation of Security Challenges. Journal of Police, General Directorate of National Security of Morocco, (42).

13. Saud, A. M. (2018). Martens Clause in International Humanitarian Law. Al Hiwar Al Mutamaddin. Article link: bit.ly/4d4pDcl

14. Ania, A. (2020). Security in Moroccan Foreign Policy. Academia Arabeia. Article link: https://bitly.ws/wp3z

15. Karim, A. W. (2021). Cybersecurity: Constraints and Challenges in Light of International Law. Article link: bit.ly/3WSUsen

16. International Committee of the Red Cross. (2019). International Humanitarian Law and Cyber Operations During Armed Conflicts. Article link: bit.ly/3WBVuu3

17. Hilali, K. (n.d.). Security Cooperation Between Morocco and the European Union. Academia Arabeia. Article link: https://bitly.ws/wPxl

18. oukal, M. (2021). A Review of the African Union Convention on Cybersecurity and Personal Data Protection of 2014. Journal of Legal and Economic Studies, Series of Publications and Works of Mohamed Bouguerra University, Boumerdes, Algeria.

19. Melih, Y. (2021). Digital Sovereignty... Manifestations and Possibilities of Achieving It in Morocco. Middle East Journal of Legal and Jurisprudence Studies, Series of Publications and Academic Works, Hassan I University, Settat, (36).

20. Qataf, S. (2022). Combating Cybercrimes in Light of International Agreements. Research Laboratory on Rights and Political Sciences, Amar Thelij University, Laghouat, Algeria. Article link: https:// bit.ly/4fzNsKC

21. Qatt, S. (n.d.). The Specificity of the Atlantic-Maghreb Partnership in the Framework of NATO's Mediterranean Dialogue. Academia Arabeia. Article link: https://bitly.ws/wph2

22. Antar, Y. (2019). Moroccan Digital Security in Light of Increasing Cyber Attacks. Moroccan Journal of International and Strategic Studies, (01).

Legal Texts

23. Law No. 05.20 on Cybersecurity, issued by Royal Decree No. 1.20.69 on Dhu al-Hijjah 4, 1441 (July 25, 2020), and published in Official Gazette No. 6904 on Dhu al-Hijjah 9, 1441 (July 30, 2020).

English references

books

24. DeLuca, C. D. (2013). The need for international laws of war to include cyber attacks involving state and non-state actors. Pace International Law Review Online, 3(9), Winter.

25. Grange, M. (2014). Cyber warfare and the law of armed conflict. Victoria University of Wellington. Retrieved from bit.ly/4dz0IgN

26. Hathaway, M., & Spidalieri, F. (2018). Kingdom of Morocco cyber readiness at a glance. Potomac Institute for Policy Studies, Virginia, United States.

Articles

27. Sipos, Z. (2023). Cybersecurity in Algeria. Journal of Security and Sustainability Issues, 13. Retrieved from bit.ly/4dcqU17.

Références en français

Ouvrages

28. BELGOURCH, A., & autres. (2020). Le cyberspace : Diversité des menaces & difficultés de régulation. Imprimerie Papèterie Elwatanya.

29. ELAZZOUZI, A. (2010). La cybercriminalité au Maroc. Impression Bishops Solutions.

Thèses

30. Rabussier, C. (2019). L'application du droit international dans le cyberespace (Mémoire de Master, Université Paris II Panthéon-Assas, Paris, France).

Articles

31. Ajijola, A.-H., & Allen, N. D. F. (2022). Leçons d'Afrique en matière de cyber-stratégie. Centre d'Etudes Stratégiques de l'Afrique. Lien de l'article: bit.ly/3YD0W2e.

32. Adriana, L. (2021). Stuxnet : Zoom sur la « cyber-arme » et comment s'en protéger. Cyberuniversity. Lien de l'article: bit.ly/4fxOYNx.

33. Bories, C. (2014). Appréhender la cyberguerre en droit international. Quelques réflexions et mises au point. OpenEdition. Lien de l'article: https://doi.org/10.4000/revdh.984.

34. Ecole d'Ingénierie Digitale et d'Intelligence Artificielle. (n.d.). Cyber-sécurité Ingénieur. EUROMED University of Fès. Lien de l'article: bit.ly/4fOJApx.

35. El Haddad, S. (2023). Digitalisation: Les universités marocaines s'engagent dans la voie de la numérisation. Maroc Diplomatique. Lien de l'article: bit.ly/3YAiXOJ.

36. Roumate, F. (n.d.). Les mécanismes légaux de lutte contre la cybercriminalité au Maroc. Lien de l'article: file:///C:/Users/hP/Downloads/adminunife,+8.+LES+M%C3%89CANISMES+L%C3%89GAUX+DE+LUTTE+CONTRE+LA+CYBERCRIMINALIT%C3%89+AU+MAROC%20(5).pdf.

37. Gery, A. (2018). Droit international et prolifération des cyber armes. Institut Français des Relations Internationales (IFRI), France, 83(2). Lien de l'article: bit.ly/4fE483V

38. Indice de Cybersécurité. (2022). Africa Cybersecurity Magazine. Lien de l'article: bit.ly/3AfIXow.

38. Jouy, M. (n.d.). Une Cyberdéfense collective en Europe? L'articulation entre cyber défenses européenne et transatlantique. Institut de Recherche Stratégique de l'Ecole Militaire (IRSEM). Lien de l'article: bit.ly/4cx7UcF.

40. Karim MISSAOUI, M., & ELHILA, A. (2021). Criminal law and ethics put to the test of cyber crime: Le droit pénal et l'éthique à l'épreuve de la cybercriminalité. Journal d'Economie, de Management, d'Environnement et de Droit (JEMED), 4(2). Lien de l'article: bit.ly/4d87j1Y.

41. M.Mouhir & Mme. Mokhtar. (2023). Stratégie de Cyber défense marocaine: du public au privé, enjeux et perspectives. Ecole de Guerre Economique. Lien de l'article: bit.ly/3WElc0M.

42. REAL,B & Francia, J. (2018). La coopération en matière de sécurité entre le Maroc et l'Europe: l'union européenne est-elle incontournable?. Lien de l'article: bit.ly/3YGeH0l.

43. SBIHI, M. T. (2021). Le droit de la cybersécurité au Maroc. LTE Magazine. Retrieved from bit.ly/4cY1uU0