Journal of Cyberspace Studies
eISSN: 2588-5502
http://jcss.ut.ac.ir
University of Tehran

Cyber Governance in Morocco: Between the Consolidation of Interne Status and the Enhancement of Global Positioning

Mhammed Kezzoute*

Moroccan Center for Cyberstudies and Security Technologies, Morocco. (*✉m.kezzoute@ump.ac.ma, https://orcid.org/0000-0001-9697-4384)

Article Info

Original Article

Main Object: Law, Moroccan Cyber Governance

Received: 07 November 2024
Revised: 23 December 2024
Accepted: 29 December 2024
Published online: 01 January 2025

Keywords:
Moroccan cyberpolicy,
Moroccan cybersecurity,
Moroccan cyber diplomacy,
Moroccan cyber governance.

Abstract

Background: The conceptualization of Moroccan cyberspace is intrinsically linked to the country's international and regional dynamics, in particular those of its African and Mediterranean neighborhood.
Aims: We open up our local experience to comparison with other known global experiences in the field of national cybersecurity, to decipher the strengths and weaknesses of national digital strategies and to fill the gaps causing the weakening of our replicating processes.
Methodology: We have mobilized quantitative techniques and potential comparative analysis to address our crucial research questions around the strengths and weaknesses within Morocco's national cyber strategy by analyzing and comparing them with other international experiences, and finally recommending best practices to maintain the regional leadership position.
Discussion: Although Morocco has acquired considerable expertise in comparison with this environment, regarding proven mechanisms of cyber stability, and the institutionalization and organization of national cyber security. However, one of the main obstacles lies in the centralization of these practices by the State, as well as in the sectorial and selective approach chosen by Moroccan policymakers to secure the national cyber space. This strategy, contrary to the country's principles of openness, was developed on the basis of the arguments, based on the priorities and strategic challenges specific to each sector.
Conclusions: The question is whether a simple reform of the central state's public policies on national cybersecurity is effective or, on the contrary, the situation requires a drastic and broader intervention, materialized by major investments and structural reforms in entire development strategies.

Cite this article: Kezzoute M. (2025). "Cyber Governance in Morocco: Between the Consolidation of Interne Status and the Enhancement of Global Positioning". *Cyberspace Studies*. 9(1): 251-272. doi: https://doi.org/10.22059/jcss.2025.385012.1114.

EISSN: 2980-9193
Publisher: University of Tehran

Cyberspace Studies, Vol 9, No 1, January 2025

1. Introduction

As an emerging nation, Morocco aims to play a leading role in cyberspace and exploit its inherent potential. This state objective is accompanied by concerted efforts and strategies to strengthen its global integration while promoting deep internal cybersecurity and cyber safety. Alongside these aspirations to build advanced technological infrastructures which Morocco expects to in these objectives, Morocco encourages government agencies contribute to this activity and seek to consolidate these guidelines by incorporating institutional and organizational frameworks to support technological initiatives and ensure a stable environment (Mastafi, 2014). Moreover, Morocco's investment in consolidating regulatory, institutional and industrial provisions demonstrates its strategic preparedness for cyber threats and evokes a national awareness of contemporary challenges and also the need for a well-defined vision and objectives.

However, constantly evolving cyber threats question the relevance of our current cyber security and national cyber stability instruments and mechanisms in the future. Our last idea is reinforced by the reality of the exponential advancement of technology and uninterrupted engagement in the digital field without tacking the evolving threats seriousness and how they have increased the vulnerability of States internationally, including Morocco as a part of this reality and also a big potential target in recent years (Bedran, 2022). Although Morocco is one of the few African countries to have made significant progress in cybersecurity and infrastructure resilience, we find that this position remains inadequate in the light of current comparative analyses, indicating a potential deficit in response to critical and dangerous situations against the nation.

2. Methodology

In this study, we will use a specific approach that combines several analysis and data collection techniques to closely examine Morocco's national cyber strategy. In this regard, we have mobilized quantitative techniques and potential comparative analysis to address our crucial research questions around the strengths and weaknesses within Morocco's national cyber strategy by analyzing and comparing them with other international experiences, and finally recommending best practices to maintain the regional leadership position.

To fully understand the debate on digital sovereignty and the geopolitics of the digital realm, we proceeded with this specific method by placing Morocco's technological autonomy in a globalized context in order to comprehend the issues of technological dependence and the challenges of technological and industrial development. To properly demystify this idea, we consulted sources containing the country's plans and strategies in the technological field, primarily Vision 2030. We also consulted Morocco's global positioning according to documents from

well-known indexes. Finally, we have targeted studies that can serve as comparative documentary sources to make comparisons in cybersecurity and cyberstrategy of advanced countries such as France, the United Kingdom, and China. The presentation of experiences and the opinions and ideas of experts and professionals serve as tools that will help us understand the state of public-private partnerships and take into account and be aware of the policies and lessons to adapt to new developments in this field.

In terms of data analysis, we have targeted themes that study governance, infrastructure, international cooperation, and education in order to theorize new factors that Morocco can use to improve its indices in alignment with global progress while also evaluating the applicability of these solutions according to the requirements of the Moroccan context. This context under discussion can, in a few terms, impose obstacles to our strategy of analysis and examination of objectives and limit the achievement of the crucial interests of this research. For further clarification, the context may cause unforeseen divergences between our objectives and Morocco's capacity to adopt such a strategy, as its socio-economic and political specificities can limit the transferability and application of the adopted strategies. But yet, we hope that following our methodology, we can ensure a thorough evaluation and examination of Morocco's digital landscape, and provide actionable recommendations and guidelines.

3. Discussion

3.1. Indices describing the national cybersecurity situation

This paragraph, will be devoted to reviewing our objective and producing a comprehensive report on the state of online cyber issues in Morocco degrading institutional and organizational achievements, taking into account international and regional dynamics. First, the relevance of the Moroccan legal framework and the effectiveness of the procedural arrangements implemented by Morocco in recent years to combat cybercrime and cyber threats should be highlighted. We will also question the ability of initiatives to mitigate technological impacts and how they can respond to their disruptions of conventional and traditional approaches to national security management, including the mitigation and degradation of the power of the State in the face of these challenges.

It is crucial to emphasize that the challenges are not merely legal or institutional, and therefore, permanent enforcement of legislation, disconnected from changes in power and influence, is not a solution in itself. Morocco must adopt a comprehensive approach to understanding the complexity and professionalism of cyber threats, consolidate its position in cyber-space pacification initiatives and strengthen the robustness of its institutions.

Furthermore, while the analysis concerns the legal framework,

diplomacy and institutional initiatives, it cannot hide the study of the country's digital infrastructures and the level of industrial and technological preparedness. These, considered to be key drivers of contemporary economies, including that of Morocco, are fundamental elements of defense strategies against cyber threats on a global scale.

3.2. The legal and institutional arsenal

Despite Morocco's position on cybersecurity consolidation, according to the ILO indicators (International Organization of Telecommunication World Index, 2016), and in relation to other States, especially the Arab States and our African counterparts, it is imperative to recognize that the progress made represents significant progress. This progress is remarkable in terms of its continental context and its Arab and North African environment, and constitutes a step forward towards the establishment of a modern and resilient national cybersecurity. (Sussman, 2019). Therefore, our analysis will focus on presenting these developments and achievements, in order to identify potential gaps and redefine, in our view, legal, institutional and legislative guidelines.

In term of legal body in recent years, the Moroccan authorities have taken important regulatory and legal initiatives. In particular, Act No. 07-03, supplementing the Criminal Code on offences related to automated data processing systems, was one of the first legislation on cybercrime in Morocco. (Direction Générale de la Sécurité des Systèmes Informatiques, 2007). Following this process, Law No. 09-08 on the Protection of Individuals with regard to the Processing of Personal Data has enriched this legal initiative by defining, inter alia, the prerogatives of the National Commission for the Control and Protection of Personal data. (Direction Générale de la Sécurité des Systèmes Informatiques, 2009). This law also structures the mechanisms associated with cross-border data transfers as well as penalties for non-compliance.

In addition, Act 53-03 on Electronic Exchange of Legal Data strengthens data protection in the context of official exchanges of information and electronic transactions, and provides the legal basis for consolidating the security of individuals in the digital space. To restore confidence in cyberspace and consolidate the rule of Moroccan law in the global digital space, other laws, such as the 05-20 Cybersecurity Act, support the national legal arsenal and strengthen its presence (Direction Générale de la Sécurité des Systèmes Informatiques, 2007). In particular, these laws establish security rules for a number of public, public and private entities, while clarifying key concepts such as cybersecurity, cyber threats and the country's vital infrastructure. (Direction Générale de la Sécurité des Systèmes Informatiques, 2020a). These laws also clearly define the responsibilities of digital actors in Morocco, while creating new entities dedicated to improving cybersecurity governance and performance.

At the domain of institutional efforts, according to the Moroccan context, the implementation of legislative initiatives can only be achieved by establishing a consolidated institutional structure that can deal with malicious innovations in the digital space and requires the necessary enforcement of legal provisions. Although the National Strategy has some ambivalence in defining its national cybersecurity priorities, it nevertheless emphasizes the importance of this harmonization and insists on its implementation as soon as possible.

As a testimony to this commitment, the Moroccan National Defense Administration has, in recent years, established two major entities. The first, the Strategic Committee for Information Systems Security, established by Decree No. 2.11.508 of 21 September 2011, is responsible for formulating the strategic guidelines on information security, and also for safeguarding the information of "sovereignty" while ensuring the proper functioning and sustainability of the information systems essential to the nation. In addition, it is empowered to validate the DGSSI action plan, to evaluate its performance, to establish the framework for IT security audits and to consult legislative and regulatory proposals inherent in IT security. The Committee under discussion is composed of prominent representatives from various public and professional spheres (Strategic Committee for Information Systems Security, 2011).

At the same time, the Directorate-General for Information Systems Security of DGSSI, established by Decree No. 2.11.509 of 21 September 2011 and affiliated with the Defense Administration, has a number of mandates aimed at strengthening the protection and effectiveness of IT systems. (Direction Générale de la Sécurité des Systèmes Informatiques, 2011).

In supplementing this institutional picture of Moroccan cybersecurity, several other entities play a leading role, namely:

- MACERT. Moroccan Computer Emergency Response Team is the security, detection and response center for cyber-attacks (Moroccan Computer Emergency Response Team, 2011).
- The NTRA, dedicated to the regulation and supervision of the telecommunications sector (The National Telecommunications Regulatory Agency, 1998).
- CNDP, ensuring compliance with personal data protection standards (National Commission, 2005).
- CMRPI, holder of the National Campaign to Combat Cybercrime (The Moroccan Centre for Polytechnic Research and Innovation, 2011).

According to the observations made, cybercrime is experiencing dramatic growth, contrary to the inertia and conservatism of the related legal frameworks and the insistence of Moroccan policymakers to continue the centralization of national cyber security instruments and

institutions (Ausim & Data Protect, 2018). This growing threat exposes Morocco to a persistent vulnerability throughout its territory, jeopardizing the relevance and effectiveness of our institutional instruments and legal and legal mechanisms, as well as our related governmental and diplomatic initiatives (Adam, 2019).

Technological developments, by complicating the nature of risks, erode the credibility of institutional approaches and related decision-making mechanisms at the national territory level and makes state initiatives incomplete. It is clear that national efforts, albeit essential, cannot be sufficient to guarantee strong and robust cybersecurity in the face of these evolving threats, making it imperative to consider a broader approach that we believe diplomacy and cooperation, aimed at harmonizing our internal efforts with existing international initiatives, can make the difference (Amrabi, 2022).

3.3. Cooperation, collaborations efforts and locales activities

In line with the approach adopted by its peers on the international stage, Morocco has engaged in a dynamic of cooperation aimed at reconciling its national competences with those of foreign specialists. Recognizing that the resilience and security of IT systems cannot be achieved in a context of security and political isolation, whose openness and cooperation have become the essential elements of cyber stability? In this regard, Morocco has integrated a clearly articulated and justified cooperation dimension into its national strategy on cyberspace, the cooperation and openness of which has been regarded as a fundamental pillar in the establishment of national cybersecurity. However, while this strategy emphasizes the importance of collaboration and the need for a structured partnership, it also advocates diversification of initiatives in order to avoid excessive concentration of efforts in a purely institutional and traditional approach.

In its aspiration to position itself on the global and regional digital scene, the Kingdom in his international cooperation strategic principle, has committed itself to anchoring itself in diplomatic and collaborative approaches that the Moroccan authorities aspire to assimilate and to leverage the know-how and expertise of their counterparts in the legal, institutional, industrial and technological fields (Mssefer, 2021). In this regard, for many years, Morocco has been actively engaged in partnerships with international organizations, states of various continents and multinational entities, all with the aim of increasing its digital resilience and achieving an adequate level of development of its core technological infrastructure.

The National Strategy on Cybersecurity emphasizes the importance of cooperation as a cardinal principle, detailing in its final chapters the parameters of this interactive approach, both from the point of view of security and industrial and technological development (National Cyber Security Strategy, 2012).

The intrinsic purpose of this cooperation is to intensify dialogue, encourage the exchange of experiences, define standards and themes of collaboration, diversify collaborating entities (universities, organizations, private sector, etc.) and develop the organizational modalities of this collaboration while cultivating fruitful relationships with public and private partners. (Mssefer, 2021). By assimilating these recommendations, Morocco is pursuing a definitive and specific path, aimed at expanding its field agreements, taking advantage of the synergies of cooperation and, at the same time, diversifying its sources of partnership and collaboration with the private sector (Lamrajni, 2023).

In the context institutional collaboration and bilateral partnership, various projects have been implemented in accordance with these partnership principles, including with Israeli, British, American and Brazilian entities. The emphasis was placed on strengthening intelligence and cooperation skills in cyberspace and improving the country's digital and technological infrastructure. With this latter mention, the orientation has clearly been towards increasing industrial and manufacturing capabilities in security and defense, cyberdefence and cybersecurity (Ministry for Foreign Affairs, African Cooperation and Moroccans Residing Abroad, 2021).

In this context, DGSSI has entered into a collaboration agreement with ANSSI, launching collaborations based on the need to establish strong links between trusted entities, while optimizing response to incidents affecting the security of information systems. These agreements codify the exchange of information, experiences and best practices between the two institutions, thereby stimulating the strengthening of Franco-Moroccan cooperation in this area. (ANSSI, 2013).

These partnerships significantly strengthen the DGSSI's competence and are part of a broader perspective to strengthen close friendship between Morocco and its strategic allies in the digital space. In addition to these bilateral collaborations, it should be noted that Morocco ratified the Budapest Convention on Cybercrime in 2018, thus strengthening its position as a pioneer of contemporary legislation at the regional level by equipping itself with a sophisticated tool to combat international cybercrime and demonstrating its use of international mechanisms of traditional cooperation (Consei de l'Europe, 2018).

Moreover, Morocco has joined the CyberSud cooperation project, as a founding member jointly with the EU and other nations such as Tunisia and Algeria. The objectives of this project include legislative consolidation, police cooperation, specialized prosecution and inter-agency security collaboration. The agreement also aims to strengthen public-private collaboration, standardize judicial training, improve international cooperation and define guidelines on cybercrime (Consei de l'Europe, 2021).

In term of locales and internes activities and with regard to training, DGSSI is committed to organizing annual international conferences and summits, bringing together researchers and specialists from various IT security disciplines, to exchange information on the latest developments in cybersecurity and to prepare relevant reports (Loudiyi, 2019). It should be noted that the roles of the DGSSI are not limited to a theoretical and analytical dimension. Indeed, the *cyberdrill* training and simulation program, orchestrated each year in conjunction with other activities, has, in its final phase, mobilized teams from various organizations and institutions to reproduce, to the extent possible, an environment simulating real operational conditions, thus subjecting participants to the tangible pressure of cyberattacks (Direction Générale de la Sécurité des Systèmes Informatiques, 2020b).

In term of specialized training and expertise transfer partnerships, since 2015, Morocco has concluded specific partnership agreements focused on the training of cybersecurity specialists with various agencies. These training sessions cover recurring and field-focused topics, including advanced technical aspects of cybersecurity, an incident management and disaster recovery course, and cyber-attack simulations, etc. (Direction Générale de la Sécurité des Systèmes Informatiques, 2022).

Adopting an alternative perspective, some researchers argue that national digital security relies more on improving the country's digital and core technological infrastructure, as well as on strengthening the nation's productive and industrial capacities, and argue, in a monopoly context, that ensuring robust national cybersecurity is conditional on increased efficiency and technological self-sufficiency in the field of cyber (Cheminat, 2021).

3.4. Performance of digital infrastructures between dependence, plans and indexations

The adoption of a paradigm oriented towards the assimilation of international experiences has undoubtedly enriched our knowledge. However, in the light of new analyses and perspectives, such efforts, although essential, no longer seem sufficient in our case. According to these advanced perspectives, the construction of a strong national cybersecurity does not depend solely on strengthening certain mechanisms and certain partnership channels or enlargement of legislative texts or diversification of the institutional heritage. On the contrary, they postulate that the primary basis of strategically reliable and resilient cybersecurity lies intrinsically in the excellence of the national technology industry, the only one that guarantees digital sovereignty and dependence alongside previous initiatives.

The paradigm adopted by China is increasingly attracting us to mention its potential by consolidating our argumentative process. China acknowledged the need to consolidate its cybersecurity capabilities

through the involvement and establishment of a strong technological and economic industrial base, while strengthening national actors (Bertrand, 2021). This policy has helped the Chinese to seize American dominance and Western technology monopoly in general. Our national strategy includes elements that deal with digital dependence and its potential impact on the overall national security landscape and on the political scene.

Nevertheless, there is still no in-depth consideration of a national initiative to revitalize and promote the national technology industry. In addition, the strategy highlights a number of areas, such as promoting national solutions in the IT security sector, supporting academic cybersecurity research, etc. However, these approaches, coupled with the gaps observed, seem insufficient for a sustainable vision of cybersecurity to meet the new challenges of cybernetism (National Cyber Security Strategy, 2012).

To go beyond certain limits, Morocco inaugurated in 2013 the project entitled Maroc Digital, a bold initiative aimed at transforming the ICT sector into an essential pillar of the national economy. Despite some criticism, it is partly thanks to these support and support arrangements that Morocco has improved its position in the international rankings in terms of connectivity, individual use and public access rates to ICTs (L'Afrique Tribune & Mazars, 2019). At the regional level, the country ranks at an honorable average in terms of the political, legal and commercial environment related to ICT and technological innovation. However, in terms of economic and social impact, the initiative has not fully achieved some of its objectives mentioned by the Moroccan Government, placing the country below average according to the same assessment criteria.

The United Nations e-Government Index highlights the stagnation in Morocco, despite the years devoted to the development of digital infrastructures and cyber technologies. The Web Index, another crucial international barometer for assessing the impact of technology on improving social, economic and political conditions, demonstrates Morocco's consistency in ICT developments (Elhamma & El-moumane, 2023). This situation prompts Morocco to optimize its position and further develop its efforts, the emergence of which in the 2020 Plan symbolizes the opening of a new era and clearly confirms the shortcomings of the previous strategy and its achievement of the objectives envisaged (Chaudier, 2014).

A detailed analysis of the indicators shows that the increase in the number of internet users in Morocco has simultaneously resulted in an increase in data and sensitive information traffic on internal networks. However, this dynamic has not been capitalized on infrastructure or human expertise, so that data from citizens or even vital actors is not fully hosted on national territory (Karkari, 2019). This issue has sparked intense debate in national security and defense circles, owing to the

problems inherent in the storage of information from citizens and sensitive institutions abroad.

So far, the resolution of this issue for Morocco can only be achieved through partnerships with foreign companies. This evokes, despite the potential benefits of openness, an underlying distrust when data management remains under the auspices of non-national actors, increasing the country's dependency and difficulties in asserting its data sovereignty (Zafagni, 2022).

The Maroc Digital 2020 plan aims to elevate the Kingdom among the technological leaders and establish it as a technological pillar at the regional and continental levels, and to fill the gaps in the previous plan. This ambition accentuates institutional, regulatory and financial pressures, exacerbated by clearly identified gaps in several areas. Nevertheless, criticism has emerged, calling this approach a precursor to technological rivalry, with Algeria, because of technological partnerships with Israel (Amouati, 2021).

This initiative could encourage the region to follow in the footsteps of Morocco, by developing its "offensive" digital capabilities, with a view to balancing the regional geopolitical situation (Mokhtari, 2021). This assertion is based on the analysis of the Chinese model which, in our view, has not only propelled the nation's technological capacity, but also generated adverse diplomatic consequences, initiating technological competition, with its neighbors and also the United States (Gendron, 2021).

We therefore demand that commitment to major technological projects serve as an indicator of a nation's strategic ambitions and may pose a danger to the neighborhood. That is why understanding issues related to cyberspace is not limited to focusing on technical, administrative or legal objectives, nor to facilitating citizens' access to the digital age. It is, in fact, a comprehensive understanding of geopolitical and geostrategic issues in cyberspace, which constitutes the fundamental element for the realization of a country’s technological aspirations (Karkri, 2019). In this regard, the Moroccan project shows an increased specificity in terms of setting new targets (Gouvernement of Morocco, 2016). It marks a significant shift from previous directives, seeking to harmonize technological ambitions with an in-depth understanding of contemporary ICT challenges (*Maghreb Arabe Presse*, 2021). In our view, this orientation reflects an awareness of the limits of the past, as well as a recognition of the challenges posed by an ever-changing global environment, which influences our diplomatic and strategic replicas.

3.5. Complexities and weaknesses of national cyberstability

Although Morocco is not below the international rankings, it remains essential to focus specific efforts to continuously optimize its positioning. It is clear, according to various indications, that a country’s

technological power and degree of digitization are intrinsically linked to its global economic, commercial, industrial and diplomatic size. Due to the many complex challenges faced by Morocco's technological ambition, the country continues to occupy ranks that may seem precarious, despite the undeniable legal and technical progress to which it is, in spite of its initiatives, behind some Arab and Asian countries that have begun their digital reforms long afterwards.

According to the ITU, Morocco ranks among the 77 nations in the digital maturity phase (Ausim, 2021). Nevertheless, the country excels in some specific areas; however, there is a clear deficit in several areas related to cybersecurity, as well as a flagrant lack of advanced technological innovations (Sauers, 2021). These gaps can be explained, in part, by the absence of major technological projects and the fragility of existing logical and material cyber infrastructures, for which the growth of a robust and competitive national cyber security industry is undoubtedly an essential lever for making Morocco an advanced country in this field, is still affected by the pretext of force majeure (Laaroussi, 2020). Nevertheless, in order to ensure a successful transition, it is imperative to fill some significant sectoral gaps and overcome persistent industrial lags (Mobarak, 2019).

3.5.1. Problem of pyramidal and non-horizontal protection

In our critical assessment of the Moroccan cyber strategy, one of the main shortcomings lies in the adoption of a sectorial approach to protection, characterized by a hierarchy based on the vital importance of the objectives to be guaranteed and secured. This national doctrine is notoriously lacking in qualitative analysis; it is limited to establishing general principles and prescribing a pyramidal defense at the expense of a horizontal structure, thus limiting itself to a limited number of agencies and institutions under the supervision of the State (Sauers, 2021).

The strategy almost completely ignores the involvement of the private sector, especially the means and small whose cybersecurity concerns are enormous. This gap is all the more worrying as these entities, although smaller, do not have insignificant areas of activity according to the same criteria of this strategy (Mobarak, 2019). Therefore, centralization of solutions is in conflict with the broader aspirations of the country, whose state monopoly on cybersecurity initiatives is discriminatory.

Experts argue that this centralization of cyber-policy places states in precarious positions when dealing with private actors that dominate these technologies (Huyghe et al., 2014).

a) Cybersecurity in the eyes of the UK, France and China

The United Kingdom, based on an inherent confidence in its private sector, explicitly recognizes its competence to regulate cyber dynamics, both nationally and internationally. At the same time, the specific actors

of this approach enjoy a valuable position, actively collaborating in the promotion and defense of the fundamental values of freedom and openness of the British cyber space. The British strategy wisely defines cybernetic boundaries, preferring ethical values to degrading measures at the expense of total openness (United Kingdom Government, 2011).

The cybernetic strategy in France revolves around targeted strengthening of industrial vulnerabilities, in terms of data storage technologies and cloud networks (Delerue et al., 2019). This model postulates that the guarantee of computer sovereignty and technological independence is based on the creation of a robust national industry independent of foreign monopoly (Coustilièrre, 2015). The Cyber Defense Pact establishes the guiding principles of this strategy, incorporating intrinsically republican concepts and an imperative of national sovereignty (Huyghe et al., 2014).

The third axis of this comparison concerns China, currently the most competitive in the world in terms of technological capacity development (Blockh, 2017). China's success in establishing a state-of-the-art industrial base has enabled it to effectively challenge the dominance of US technology companies (China Initiative Strategy Report, 2021). In this context, strengthening the presence of domestic technology operators and their positioning in global competition is a national priority in China (Jinhua, 2019).

This comparative analysis reveals that these nations have given priority to the specific strengthening of their infrastructure and the competitiveness of their national players before committing to the international. They see national capacity-building as a prerequisite for expanding external commitments, building on existing programs that promote the domestic interests and objectives of their national policymakers to the detriment of international fairness (Stauffacher & Weekes, 2012).

As a result, these countries adhere to strategies that incorporate less transparent aspects, recognizing that the overall security of a country depends primarily on building specific capacities in cyberspace. And they suggest that the guarantee of national security is based on the development of technological, industrial and military potential who's developed IT capabilities should not be the monopoly of certain bureaucratic sectors at the state central level (Iraqui, 2014). To this end, we are advocating a new Moroccan vision of cyberspace that combines the benefits of these strategies by sharing the benefits among all internal actors.

b) Selective security in the face of a growing global threat

We address the omnipresent and multidimensional nature of cyber threats, while highlighting the selective and sectorial aspect of the Cyber Security Strategy in Morocco. Despite the ubiquity of cyber threats, this strategy presents a significant disparity in homogeneity, evident even in areas

identified as critical. This selectivity is increasing due to budgetary constraints and human resources, hindering the progress of the digitization initiative in some key sectors (The National Telecommunications Regulatory Agency, 2020). Paradoxically, it is imperative to note that measures to improve cybersecurity will vary significantly from one functional area to another according to criteria and capabilities.

It should be noted that cross-sectoral dissonance fuels the observable decline in overall national cybersecurity performance. Indeed, the locomotive model, where a highly secure and developed sector should stimulate the less developed regions, is counterproductive from our point of view. This approach is already exhausting limited resources in the area of cyber security and cyber defense, rather than promoting operational synergies. It is also believed that these consequences, coupled with territorial development inequalities in Morocco, hinder the expansion of cybersecurity at the national level, which, in our view, is inseparable from issues relating to territorial and social development in general and cannot be reduced to a mere technical problem.

The legal sphere is not without challenges. There is a certain legal hegemony, where Moroccan legislation often neglects the jurisprudential innovation in favor of the adoption of mainly French-speaking roads. This approach inhibits the ability to anticipate and understand the ever-evolving cyber challenges in Morocco and in accordance with Moroccan specifics. The digital space therefore requires a major reorientation of national policies in order to the desired objectives. Finally, recent economic and health crises have highlighted the crucial importance of digital as a resilience tool to global challenges (Amadeus Institute, 2020), whose maximization of its effectiveness, is imperative to remove the sectoral and territorial barriers that hinder its development (Coustilièrre, 2015).

c) The geostrategic importance of technology industries

In the first part, we identified the crucial importance of ICTs and highlighted their negative repercussions, thereby strengthening their position in the strategic paradigms related to geopolitical confrontations and struggles (Mussington, 2021). It must be reaffirmed that the military and security importance of these technologies has not increased in political and strategic areas without reason; but because, the global economy and global industry have become central players in this economic and industrial war for the acquisition and control of technological potential (Partik & Mishra, 2022).

The most appropriate example is the rivalry between China and the United States, which is no longer just a struggle for global supremacy, but also for economic, industrial and, above all, technological dependence. This country aspires, through this competition, to ensure the primacy of its industries while guaranteeing China’s technological sovereignty in cyberspace. (Dufour, 2021).

Nations with proven cyber power are fully aware that the robustness of their cybersecurity is predominantly determined by the industrial growth of national security-related technologies (Gendron, 2021). This element is the only guarantee of genuine independence and cyber sovereignty for which Morocco, in this context, aspires to take advantage of the economic rivalries between the great powers in the field of technology in order to attract the necessary investments for the development of its infrastructure and its technological sector.

In this regard, the deployment of infrastructure projects has been the subject of various initiatives, and the country's new industrial and technological capacity-building plan includes in its body an ingenious strategy and an innovative plan, provided that it has the necessary resources to monitor and promote small technological enterprises (Idrissi, 2020).

Designed in collaboration with the private sector (El Maataoui & Laamir, 2022), this plan represents a coherent national road map for the development of the national ICT industry and offers an opportunity for substantial private sector participation in this industrial and technological transformation (Kabbaj, 2017). The various construction sites that make up this strategy may seem excessively ambitious and are not necessarily equipped with adequate funding mechanisms and governance structures. This is undoubtedly an important step that professionals in the sector must take into consideration in order not to reap the same results as previous plans. Indeed, the challenges in the ICT sector are enormous and, despite some progress, our country is experiencing growing differences from other nations.

For example, Turkey devotes 1.7% of its national budget to IT, 2.7% of private spending, 11 engineers per 10,000 inhabitants, and has more than 15 companies that generate a turnover of more than EUR 100 million, which serves as a driving force for the ecosystem of IT players. Morocco, on the other hand, has 0.8%, 1.4%, 3 engineers and no company exceeds the EUR 1 million threshold (ibid).

The challenge is therefore tangible: it is imperative that Morocco equips itself with the necessary capabilities to elevate its position in accordance with the ambitions set out in this new plan and thus become the leading technological hub on the African continent (Najah, 2020).

d) Revision of education policy

Depending on the view that several elements strengthen or weaken national strategies, the presence or absence of the educational element in an IT strategy constitutes a turning point in our study case. Moroccan public policy in the field of cybersecurity still risks ignoring the role of education and the importance of having specific plans in education or even outside educational institutions related to issues related to cyberspace (Sauers, 2021).

We would like to highlight the absence of specific education and

awareness-raising programs on the study and analysis of cybernetic issues from a broader and broader perspective, aimed at better understanding the challenges and challenges in this field in the social science vision. Furthermore, we seek to keep instruction and teaching of cybernetic issues and technological challenges as far away as possible from the exclusive domain and privilege of the elites, and to make this science an open and popular area of access (Yoann, 2019).

This task can only be achieved through the sharing of technological knowledge according to a paradigm of awareness-raising and sensitization of citizens and entities concerned. We mean that, for the democratization of cyber awareness and the sharing of knowledge around cyber threats that are becoming increasingly professional and more complicated, will only be achieved with the adoption of specific and official programs and that mobilize the necessary capacities to reduce the effects of the cyber-threats and also the impacts yet unknown

3.6. A deeper analysis of national situation

To clarify our critical viewpoint, we demonstrate in the following paragraphs the interrelations and probable implications after examining the legal and institutional framework, as well as anticipating the geopolitical dimensions of international cooperation in this aspect of the debate. For this reason, we confirm that the legal advancements in the field of cybersecurity in Morocco indicate relevance and progress, providing comfortable positions for our situation. However, we simultaneously note deficits in implementation and coherence. Most of the laws surrounding cybercrime in Morocco provide robust and deterrent frameworks against the spread of malice within the network, yet the implementation of a specific inter-agency collaboration mechanism will always remain a demand (Mobarak, 2019). This gap will prolong the shortcomings and keep the jurisdictional field far from national ambitions. That is why we have adopted external experiences and lessons, emphasizing the importance of introducing lessons and experiences from the private sector to give a new judicial spirit to national and local perspectives. The introduction of new practices and applications can help the Moroccan legal structure adapt to international and intercommoned advancements aimed at countering cyber threats.

Regarding the institutional framework, it is important to note that institutional efforts place Morocco on par with legal efforts, and prestigiously within its regional context. The creation of national agencies and institutions for the management and cybersecurity of core computer systems constitutes a significant step forward in affirming the country's presence in the field of international cybersecurity. However, it seems that these efforts are not at the level of ambitions and the evolution of the cyber threat towards cross-border levels. According to our analyses, this constitutes a centralization of national cybersecurity that risks not only gathering security and defense power at a single

central level but also ignoring the decentralization of cybersecurity as some experiences suggest. On the contrary, this confirms the Moroccan state's intention to continue marginalizing the role of the private sector and its contributions in the implementation of transnational cybersecurity strategies and plans, as well as the continued disregard for territorial and local specificities between the country's regions (Sauers, 2021). For this reason, we emphasize the importance of finding a balance between all these issues in order to achieve a strategy for decentralizing cybersecurity governance that includes all concerned parties and integrates the private sector, as the existence of a participatory approach could resolve structural inefficiencies and promote a more inclusive cybersecurity ecosystem (Huyghe et al., 2014).

4. Conclusion

We concluded this study by saying that Morocco is probably a competing country in the field of cyber institutionalization and governance by comparing it with its geographical environment and his positioning as a third world state. The country has established the core institutions in cyber threat governance and national cybersecurity and also has reinforced the legislative framework, whose neighbors, especially African countries and Arab counterparts, still face difficulties in establishing such resilience despite the financial and organizational capabilities deployed by those countries in discussion.

We would also like to point out that during our analysis process, we have identified some weaknesses and shortcomings in Moroccan efforts to higher levels in cybersecurity compared to some leading countries in the field at the international level, even if Morocco has recently occupied a very honorable position among the 40 countries which have the best international conditions in cybersecurity. In this regard, we have recommended a number of reforms to be adopted and introduced into administrative and governmental processes especially the consideration of the roles of all the others non state actors in new cyber diplomacy, in order to bring national cybersecurity to full performance in the face of the rise in power of cyber-attacks and occupational cyber threats.

Nevertheless, we note that the recent reforms established by the inauguration of the 2030 Cyber Strategy Vision reveal several hopes and aspirations whose policymakers believe to reach the effective levels for the establishment of national cyber resilience in cyberspace and at the same time address the new trends and emerging issues in cyberspace more effectively.

In terms of geopolitical implications, Morocco's positioning as a leading country in the region exposes, as we claim, vulnerabilities and pressures against the general security system. The innovative partnerships that the country has recently engaged in, especially those

with China or Israel, positively impact the development of security and defense technologies. However, they also pose challenges of technological dependencies on external actors and, more seriously, tensions with regional or even international powers. In this regard, we have alarmingly noted in our study how technological alliances can, in certain cases, prompt other actors, especially states, to intervene and meddle in the affairs of another state to steer it away from these paths. This power play is currently underway and reflects how the dynamics of power intertwine with technological competition and geopolitical rivalry, providing the most concrete example on the global stage, which is that of China and the United States (Partik & Mishra, 2022). So, for Morocco to find a balance between these imposed challenges and its national objectives, it should establish a strategy that combines national ambitions to maintain digital and technological sovereignty with the need to acquire international expertise. This is only achievable by preventing the geopolitical repercussions caused by such collaboration or partnership while simultaneously contributing to the emergence of a robust and future-ready cyber strategy that takes into account our internal specificities and respects our international commitments.

To strengthen this process, it is also crucial to give importance to public-private partnerships, of which Estonia's e-governance model illustrates the success of such an approach. In the same vein, there are numerous initiatives that can serve as examples, such as the case of South Korea in strengthening technological and security capabilities under the public-private partnership model and how they have made significant progress in development and national security. This model, if adopted by Morocco, will help planning authority’s secure sufficient funding resources, which currently hinders the implementation of several national projects promoting technological dependence.

Technological dependence is often under pressure due to the importation of sophisticated services and IT tools, with over 70% coming from China. This raises questions about the security and sustainability of international supply chains and the obligations of exporting states towards their clients in the event of a crisis or disaster (Baldwin et al., 2021). This, on the one hand, sheds light on the relativity and limitations of partnership solutions and compels us to recognize the necessity of having a national industrial base in this vital and strategically important field, which is the technological domain. India, in this regard, illustrates the most innovative example for Morocco in terms of digital sovereignty, maintaining technological dependence by launching an ambitious national program called "Make in India", which aims to reduce dependence on foreign suppliers and encourage domestic production in all fields, including the technological sector (Gupta & Jawanda, 2020).

For further example, the Republic of Rwanda is also adopting an initiative for its rapid digital transformation in a context with very

limited resources and skills. But, thanks to strategic investments in connectivity infrastructure, the country has managed to secure perfect positions and achieved an impressive ranking among the top twenty countries in the world in just five years. This plan from Rwanda has helped decision-makers in the country not only to improve the level of cybersecurity but also to reduce social disparities between the regions of the country and territorial inequalities, which Morocco can take measures to reduce regional disparities and fill gaps in community ICT programs.

Conflict of interest

The author declared no conflicts of interest.

Ethical considerations

The author has completely considered ethical issues, including informed consent, plagiarism, data fabrication, misconduct, and/or falsification, double publication and/or redundancy, submission, etc. This article was not authored by artificial intelligence.

Data availability

The dataset generated and analyzed during the current study is available from the corresponding author on reasonable request.

Funding

This research did not receive any grant from funding agencies in the public, commercial, or non-profit sectors.

References

Adam, J. (2019). "Cybersécurité: Encore trop de fragilités". *Journal l'Économiste*. https://www. leconomiste.com /article/cybersecurite-encore-trop-de-fragilites.

Amadeus Institute. (2020). "Rapport complémentaire, Adaptation, innovation, agilité, créativité et efficacité: Les 5 piliers de la relance et de la construction du modèle de développement national Post-Covid-19". https://www.admin.amadeusonline.org/app/uploads/2021/01/RA2020-175x250-1.pdf.

Amouati, R. (2021). "Câbles optiques sous-marins: Le Maroc sera raccordé à Ella Link". *Journal Tic Maroc*. https://www .tic-maroc.com.cables-optiques-sous-marin-le-maroc-sera-raccorde-a-elllalink.

Amrabi, S. (2022). "Cybersécurité : Un marché stratégique où tout reste à faire". *Journal l'Opinion*. https://www. Lopinion.ma/Cybersecurite-Un-marche-strategique-ou-tout-reste-a-faire

ANRT. https://www.anrt.ma/lagence/presentation.

ANSSI: Agence Nationale pour la Sécurité Nationale. (2013). "Sécurité des systèmes d'information : la France et le Maroc signent un accord de cooperation". https://cyber.gouv.fr/publications/securite-des-systemes-dinformation-la-france-et-le-maroc-signent-un-accord-de.

Ausim Maroc (2021). "Le livre blanc : les enjeux de la cybersécurité au Maroc". *Bibliothèque Nationale du Royaume*. https://www.ausimaroc.com/wp-content/uploads/2018/10 /LB-Les-enjeux-de-la-cybers-au-Maroc.pdf.

Ausim & Data Protect. (2018). *Les Enjeux de la Cybersécurité au Maroc*. Bibliothèque Nationale du Maroc.

Baldwin, R.; Freeman, R.; Miroudot, S.; Theodorakopoulos, A. & Grossman, G. (2021). "Risks and global supply chains: What we know and what we need to know". 29444. https://www.nber.org/system/files/working_papers/w29444/w29444.pdf.

Bedran, M. (2022). "Menace terroriste sur le cyberespace marocain". *Aujourd'hui le Maroc*. Mai 11. https://www.aujour_dhui.ma/societe/menace-terroriste-sur-le-cyberespace-marocain.

Bertrand, M.A. (2021). "La recherche d'une souveraineté numérique en Russie: à qui profite-t-elle?". *La Revue Géopolitique Diploweb*. https://www.diploweb.com/La-recherche-d-une-souverainete-numerique-en- Russie- .

Blockh, L. (2017). "Géopolitique du cyberespace, nouvel espace stratégique: l'internet, vecteur de puissance des Etats-Unis?". *La Revue Géopolitique Diploweb*. https://www.diploweb.com/-L-Internet-vecteur- depuissance-des-Etats-Unis-.

Chaudier, J. (2014). "La stratégie Maroc Numérique 2013 a échoué". *Econostrum*. https://www.econostrum.info/La-strategie -Maroc-Numeric-2013-a-echouea.html.

Cheminat, J. (2021). "La NSA injecte des backdoors dans les matériels IT à l'export". *Journal Silicon*. https://www.silicon.fr/nsa-injecte-backdoors-les-materiels-it-lexport-94308.html#.

China Initiative Strategy Report. (2021). *China as a 'cyber great power': Beijing's two voices in telecommunications*. https://www.brookings.edu/articles/china-as-a-cyber-great-power-beijings-two-voices-in- telecommunications/.

Consei de l'Europe. (2021). *Projet CyberSud – Coopération en matière de cybercriminalité dans la région du Voisinage Sud*. https://south.euneighbours.eu/fr/project/projet-cybersud-cooperation-en-matiere-de- cybercriminalite-dans-la/.

----------. (2018). "Le Maroc adhère à la Convention de Budapest sur la cybercriminalité et à son Protocole sur la xénophobie et le racisme". https://www.coe.int/fr/web/cybercrime/-/morocco-joins-the-budapest-conventionon-cyber crime-an-becomes-it-s-60th-member- .

Coustilièrre, A. (2015). "Maîtriser le combat dans l'espace numérique et contribuer à la sécurité numérique nationale". *Revue de la Géoéconomie*. 75(3): 25. http://dx.doi.org/10.3917/geoec.075.0025.

Delerue, F.; Deforges, A. & Géry, A. (2019). "A close look at France's new military cyber strategy". *Center of Security Studies.* https://www.Isnblog.ethz.ch/a-close-look-at-frances-new-military-cyber-strategya-close-look-at-frances-new-military-cyber-strategy.

Direction Générale de la Sécurité des Systèmes Informatiques. (2022). "Cycle de formation en cybersécurité – partenariat DGSSI/ OTAN". https://www.dgssi.gov.ma/fr/content /cycle-deformation-en-cybersecurite-partenariat-dgssi-otan.html.

----------. (2020a). "LOI 05.20 Relative à la cybersécurité". Bulletin Officiel, n 6906, 06-08-2020. https://www.dgssi.gouv.ma/fr/content/loindeg0520relativelacybersecurite.Html.de20d'Information.

---------- (2020b). https://www.dgssi.gov.ma/fr/presentation/dgssi/presentation-missions.html.

----------. (2011). "écret n 2-11-509 du 22 chaoual 1432 (21 septembre 2011) complétant le décret n 2-82-673 du 28 rabii i 1403 (13 janvier 1983) relatif à l'organisation de l'adn et portant création de la dgssi | DGSSI. (n.d.). https://www.dgssi.gov.ma/fr/decret-ndeg2-11-509-du-22-chaoual-1432-21-septembre-2011-completant-le-decret-ndeg.

----------. (2009). LOI 09-08, Relative à la protection des personnes physiques à

l'égard du traitement des données à caractère personnel. Bulletin Officiel. n° 5714. March 05. https://www.dgssi.gov.ma/fr/content/loi-09-08-relative-la-protection-despersonnes-physiques-l-egard-dutraitement-des-donnees-caractere-personnel.

----------. (2007). "LOI 53-03 Relative à l'échange électronique des données juridiques". Bulletin Officiel. 5584. 06-12-2007. https://www.dgssi.gouv.ma/sites/default/files/attached_files/loi3-05fr-new.pdf.

Dufour, F.J. (2021). "Entre la Chine et les Etats-Unis, la guerre technologique a toutes les chances de se poursuivre". *Journal le Monde*. https://www.lemonde.fr/idees/article/entre-la-chine-et-les-etats-unis-la-guerretechnologique-a-toutes les-chan ces-de-se-poursuivre.html.

El Maataoui, R. & Laamir, J. (2022). "La Digitalisation et la Productivite des Entreprises au Maroc : Etude d'Impact à l'Aide de la Methode de la Propensity score Matching". *Journal of Social Sciences & Organization Management*. 3(2): 17. https://doi.org/10.48434/IMIST.PRSM/jossom-v3i2.34851.

Elhamma, A. & El-moumane, R. (2023). "Impact de la taille sur la digitalisation du contrôle de gestion des entreprises marocaines: Résultats d'une enquête". *Alternatives Managériales Economiques*. 5(3): 182-199. https://revues.imist.ma/index.php/AME.

Gendron, G. (2021). "Les semi-conducteurs : clé de l'autosuffisance technologique chinoise". *Chroniques de Nouvelles Conflictualités de la Chaire Raoul Dandurand*. https://dandurand.uqam.ca/wp- content/uploads/2021/02/2021-02-09_semi-conducteurs_Gabrielle.pdf.

Gouvernement of Morocco. (2016). *Le Maroc gagne deux places dans l'indice mondial de l'UIT*. https://www .egov.ma/fr/actualites/le-maroc gagne-deux-places-dans-lindice-mondial-de-luit.

Gupta, S. & Jawanda, M.K. (2020). "The impacts of COVID-19 on children". *Acta Pédiatrique*. 109(11): 2181-2183. https://doi.org/10.1111/apa.15484.

Huyghe, B.; Kempf, O. & Mazzucchi, N. (2014). "La composantes politico-militaire, économique et sociétale d'une cyberstratégie française: agir dans la dimension sémantique du cyberspace". *Rapport final de l'Institut de Relations Internationales et Stratégiques*. 24. https://www.iris-france.org/wp-content/uploads/2017/06/csfrs_resbat_rapport_final.pdf.

Idrissi, J.I. (2020). "La transformation digitale des PME au Maroc: Enjeux et perspectives". *Revue Repères et Perspectives Economiques*. 4(2): 198-211. https://doi.org/10.34874/IMIST.PRSM/RPE/21539.

Iraqui, F. (2014). "Télécoms: le Maroc perd le fil". 360. https://fr.le360.ma/economie/telecoms-le-marocperdle-fil-26197.

Jinhua, L. (2019). "What are China's cyber capabilities and intentions?". *Carnegie Endowment for International Peace*. https://carnegieendowment.org/posts/2019/04/what-are-chinas-cyber-capabilities-and-intenti ons?lang=en.

Kabbaj, O. (2017). "La création de l'Agence nationale pour le développement numérique suscite beaucoup d'espoirs chez les professionnels marocains". *Journal Telquel*. https://telquel.ma/2017 /08/02/la-creation- de-lagence-du-developpement-numerique-officialisee-par-le-parlement_1556251.

Karkri, S.B. (2019). "Le Maroc la future digital nation de l'Afrique". *L'Afrique Tribune, Policy Paper*. 11. https://static.latribune.fr/1207516/le-maroc-la-future-digital-nation-africaine.pdf.

Laaroussi, N. (2021). "Cybersécurité: menaces et enjeux". *Journal l'Opinion*. https://www.lopinion.ma/Cybersecurite menaces-et-enjeuxa.html.

L'Afrique Tribune & Mazars. (2019). "Le Maroc la future digital nation de l'Afrique". 1-36. https://static.latribune.fr/1207516/le-maroc-la-future-digital-nation-africaine.pdf.

Lamrajni, M. (2023). "Maroc – République de Corée : Comment Séoul veut devenir un partenaire stratégique de Rabat". *Journal l'Opinion*. https://www.lopinion.ma/Maroc-Republique-de-Coree-Comment-Seoul- veut-

devenir-un-partenaire-strategique-de-Rabat_a44676.html.
Loudiyi, A. (2019). “7 ème édition du séminaire sur la cybersécurité organisée par la Direction Générale de la Sécurité des Systèmes d'Information”. https://www.dgssi.gov.ma/fr/content/discours-de-monsieur-le-ministre-l-occasion-du-7eme-seminaire-sur-la-cybersec urite.html.
MACERT. https://www.dgssi.gov.ma/fr/macert
Maghreb Arabe Presse. (2021). "L’African Super Computing Center, une infrastructure de pointe pour le renforcement des liens entre la recherche et l’industrie". February 19. https://www.mapnews.ma/fr/benguafricansupercompuenter-une-infrastructure-de-pointe.
Mastafi, M. (2014). "Obstacles à l’intégration des technologies de l’information et de la communication (TIC) dans le système éducatif marocain". *Frantice Net.* 1(8): 50-65. http://www.frantice.net/index.php?id=870.
Ministry for Foreign Affairs, African Cooperation and Moroccans Residing Abroad. (2021). “Morocco and Isreal sign three cooperation agreements”. https://www.diplomatie.ma/fr/le-maroc-et-isra-signent-trois-accords-decoopA9ratio.
Mobarak, L. (2019). "Diagnostic Stratégique de l’émergence économique du Maroc, Éd". *The Policy Center for the New South.* https://www.policycenter.ma/sites/default/files/2021-01/PP19-19MoubarackLo0.pdf.
Mokhtari, R. (2021). “La question cyber-sécurité, un défi de taille pour nos Forces Armées”. *La Nouvelle République*. https://www.lnr-dz.com//la-question-cyber-securite-un-defi-de-taille-pour-nos-forces-armees/.
Mussington, D. (2021). "Strategic stability, cyber operations and international security". *Center For International Governance & Innovation*. https://www.cigionline.org/articles/strategic-stability-cyber-operations- and-intern ational-security/.
Mssefer, D. (2021). "Les enjeux de la cybersécurité au Maroc". *Journal la Conjoncture*. 22-26. https://www.cfcim.org/wp-content/uploads/2021/12/1041-novembre-2021-Cybersecurite.pdf.
Najah, R. (2020). "Le cyberespace Africain : un état des lieux". *Policy Center for the New South*. https://www .Policycenter.ma/opinion/le-cyberespace-africain-un-etat-des-lieux.
National Cyber Security Strategy. (2012). https://www.dgssi.gov.ma/en/publications/national-cybersecurity-strategy.
The National Telecommunications Regulatory Agency. (2020). *Enquête annuelle sur le marché et l’évolution des TIC, «Marché des Technologies de l’Information*. http://www.anrt.ma/indicateurs/etudes-et-enquetes/enqueteannuelle-marche-des-tic.
Partik, S. & Mishra, V. (2022). "Democracy, Technology, Geopolitics". *Observer Research Foundation*. https://www.orfonline.org/expert-speak/democracy-technology-geopolitics/.
Sauers, M. (2021). “Global Cybersecurity Index 2020 Ranks Morocco at 50th Globally”. *Morocco World News*. https://www.moroccoworldnews.com/global-cybersecurity-ranks-morocco.
The Strategic Committee for Information Systems Security. (2011). https://www.dgssi.gov.ma/fr/presentation/csssi/missions-du-comite-strategique-de-la-securite-des-systemes-d- information
National Commission. https://www.cndp.ma/qui-sommes- nous/commision.html
Stauffacher, D. & Weekes, B. (2012). "The challenge of protecting critical infrastructure against Cyber-Attacks". *Center for Security Studies*. https://www.files.ethz.ch/isn/188471/ISN 154200en.pdf.
Sussman, B. (2019). “The List: best and worst countries for cybersecurity”. *The Secure World News Team*. Novembre 13. https://www.secureworldexpo.com/industry-news/countries-dedicated-to-cybersecurity.

United Kingdom Government. (2011). *The UK cyber security strategy protecting and promoting the UK in a digital world*. https://www.gov.uk/government /news/protecting-and-promoting-the-uk-in-a-digital-world--3.

Yoann, N. (2019). "Pourquoi l'éducation à la cybersécurité est-elle importante?". *Journal of Cybersecurity Guide*. https://www.cybersecurity-guide.com/pourquoi-leducation-a-la-cybersecurite-est-elle- importante/.

Zafagni, M. (2022). "Les Etats-Unis bannissent les équipements Huawei et ZTE en invoquant un risque pour la sécurité nationale". *CENT France*. https://www.cnetfrance.fr/news/les-etats-unis-bannissent-les- equipements-huaweiet-zte-en-invoquant-un-risque-pour-la-securite-nationale-9950406.