STAP
Smart Technologies Academic Press

Journal of Cyber Security and Risk Auditing

https://www.jcsra.thestap.com/

JOURNAL OF CYBER SECURITY AND RISK AUDITING
Smart Technologies Academic Press
STAP

# Cyber Intelligence and Moroccan National Security: What Strategy for Managing and Mitigating Cyber Threats against Future Sporting Events

**Kezzoute Mhammed** [1]

[1] *Founder & Director of the Moroccan Center of Cyber studies & Technologies Security, Morocco*

## ARTICLE INFO

**Article History**
**Received:** 17-05-2025
**Revised:** 10-08-2025
**Accepted:** 15-09-2025
**Published:** 19-09-2025

**Vol.2025, No.1**

**DOI:**
https://doi.org/10.63180/jcsra.thestap.2025.4.12

***Corresponding author.**
***Email:***
*m.kezzoute@ump.ac.ma*

**Orcid:**
https://orcid.org/0000-0001-9697-4384

## ABSTRACT

Cyber intelligence currently presents itself as a key solution to strengthen cybersecurity practices and the resilience of vital infrastructures. For this, in our study, we explore the interactions between this new concept and national security, as well as the existing frameworks organizing national cybersecurity in the face of the rise of mutating and transformative cyber threats. Critiquing the existing frameworks, we hope to provide effective recommendations in existing legislation and regulatory frameworks, in funding methods, in modalities of international cooperation and collaboration, and in the development of key technologies and industries in this process, to overcome the current gaps and voids in the critical situation and strengthen measures for better national cybersecurity. Based on previous experiences regarding the application of these practices in conjunction with technologies to strengthen our argumentation process, we have observed that these measures are essential and important for the consolidation and securing of critical digital infrastructures and the preservation of cyber sovereignty, especially those that are aligned with international standards and technological advancements in cyber stability. For this reason, we call in this study for additional re-search on Morocco's National Cyber Strategy for 2030, exploring the possibilities of strengthening national cybersecurity against evolving cyber threats through the integration of cyber intelligence into detection, analysis, and decision-making pro-cesses.

**Keywords:** Moroccan Cyber Strategy, Moroccan Cyber Policy, Moroccan Smart cities, Cyber Governance, Cyber Security.

**How to cite the article**
Mhammed, K. (2025). Cyber Intelligence &amp; Moroccan National Security: What Strategy for Managing and Mitigating Cyber Threats against Future Sporting Events. Journal of Cyber Security and Risk Auditing, 2025(4), 366–383. https://doi.org/10.63180/jcsra.thestap.2025.4.12

## 1. Introduction

Morocco has experienced a massive technological transformation in recent years, accompanied by the introduction of IT development strategies and the large-scale implementation of significant digital devices. This relentless evolution, accompanied by the adoption of specific planning such as the intelligent management of Smart cities and the development of critical and essential urban infrastructures through technologies and devices, not only constitutes a strong point for the country's advancement in the field of urban cities and in the global indexing concerning the country's IT development [1].

Conversely, it constitutes the basis on which cybercrime continues to target Morocco due to the massive and continuous expansion of the national digital network in terms of opportunities to exploit for achieving their criminal objectives. In this regard, the cybercrime we aim to address in our study and that we believe we will confront, goes beyond the level of gain or personal satisfaction objectives, where the presence of instigation logic allows cybercriminals to carry out their activities under the aegis or collaboration with a foreign service for large-scale disruption objectives or to inflict damage against national security.

Alongside the colossal digitization projects that Morocco is undertaking, which present an opportunity for cybercriminals to achieve their objectives, the Moroccan State's commitment to the intelligent management and planning of crises, where the overload in digital service infrastructures accumulates gaps and needs, can also be exploited by criminals to increase their online malicious activities. Fraud, phishing, data and identity theft, etc., as the indicators suggest—justifying our vision—have increased during the COVID crisis, which the Moroccan state tried to control in terms of scale and undesirable impacts through still modest digital devices in 2020[2].

The situation alarmed decision-makers about the level of cybersecurity in the case of such events, which is still low and far from Morocco's ambitions despite efforts to develop and deploy digital technologies on Moroccan territory. In addition to the above, such events increasingly attract highly skilled cybercriminals with diverse backgrounds, ranging from simple criminal activities to extreme conspiracy and large-scale disruption[3]. The situation, then, is still vulnerable and requires increased vigilance and the presence of a defined policy as well as a concrete cybersecurity strategy for digital infrastructures concerning the organization and management of such large-scale events, especially since Morocco will host major and important international sporting events in the coming years.

This vulnerable situation that we are trying to demonstrate serves as the starting point to justify the importance of the presence of such a concept of intelligence in cyberspace as an essential element for strengthening Morocco's preventive cyber-security during the organization of international sporting events. With the help of technological devices, especially those used in urban planning processes, such activities improve the level of vigilance by providing more advantages for the preventive detection of online malice through proactive evaluation of massive data and the identification of suspicious actors in order to avoid such negative impacts and magnitudes. Moreover, these processes are necessary as the development of information technology in Morocco is essentially linked to the creation of value and the growth of economic and commercial services, including public security and stability. This justify for us the presentation of this concept of intelligence in cyberspace as a necessity in order to protect important digital infrastructures during the events under review. Reinforcing the process of justifying the importance of these practices, we have also consulted several studies on this topic that advocate for the necessity of the existence of intelligence in cyberspace to improve the security of smart urban cities. And we found that the presence of advanced online surveillance and the massive control of data and the flow of traffic in the digital network, as well as the analysis of the gathered data using the potential of artificial intelligence, currently as Chouraik (2024) confirm, constitute the cornerstone in strengthening policies and strategies for preventing online cybercrime in several countries.

In parallel with the processes of establishing digital infrastructures, Morocco has engaged in similar processes to strengthen and establish cybersecurity and cyber stability. Numerous institutions of cyber governance and establishments for strengthening national security measures in cyberspace have been put in place, including ma-CERT, GDSIS, and GCSIS, in addition to several other state bodies that address IT challenges by providing responses, explanations, and awareness regarding incidents related to cyber threats[4]. The Moroccan Urgent Response Center, the Directorate, and the General Committee for the Security of Computer Systems all constitute the starting point for Morocco to strengthen national cybersecurity.

It also demonstrates an exceptional willingness regarding investment in advanced surveillance technologies, especially in the satellite domain, indicating to us that the country generally gives exceptional priority to security, intelligence, and control operations [5]. However, we noted that the level of adaptation between the processes of introducing technologies into daily activities such as services, administration, authority, urban planning, security, and defense, etc., still risks being hindered in the face of the processes of developing cybersecurity policies and strengthening the mechanisms and application devices, making the need for a specific strategy imperatively essential.

The fact that Morocco will engage in organizing major international events in the near future will not change its increasing exposure to cyber threats. However, the situation will encourage cyber challenges to transform in order to maximize the impact on the security of infrastructures and the stability of sports services. For this reason, the implementation of a special strategy and a concrete and valuable approach to the strategic cybersecurity challenges of international sporting events is urgent in order to secure and stabilize the conduct of these global events. Summarizing the necessity of such an approach, we see that the anticipated framework of this specific strategy should take into consideration the political stakes surrounding the organization of these events, the technological innovations used by online criminals, and finally the collaborative and cooperative aspect with international actors of different natures, already experienced in this kind of activities.

We see at the core of our requirements that the cyber challenges within the sporting events that Morocco will organize in the coming years range from low-scale cyberattacks to large-scale cyberattacks against digital infrastructures and against participating individuals, spectators, and all other national assets.

The implementation of such a strategy should commit to respecting certain specific aspects, which we believe include prioritizing the protection of vital digital infrastructures, strengthening intelligence mechanisms in cyberspace, consolidating surveillance and online control measures, improving governance frameworks and regulatory and legal frameworks regarding the organization of such events, and promoting awareness of cyber challenges during these events, as these will be assets for successfully managing these occasions. In this context, we also note that promoting public-private intergovernmental collaboration, including with international organizations specialized in the field of cybersecurity, in order to over-come the undesirable impacts of cyber threats, will be an opportunity for Morocco to overcome this critical situation. Morocco, by trying to provide more concrete responses to the cyber challenges related to the organization of such events, will demonstrate to the world the broader implications of cybersecurity and also what new experiences are needed to successfully organize these events.

According to this presentation, we are trying in our study to theorize the strategic measures that Moroccan decision-makers need to overcome the critical situation when organizing such an event threatened by hackers. The evaluation and examination of similar events, the analysis of existing identical cyberattacks, and finally the monitoring of intelligence expertise operations in cyberspace will help us provide the necessary proposals regarding the specific strategy desired and con-tribute to the establishment of a robust and relevant national framework for the cybersecurity of international sporting events.

## 2. Overview of Cyber Threats in Morocco

Digital transformation in Morocco has improved the country's ranking in international classifications related to IT development and technology adoption and its introduction into various aspects of human life. However, these technological advancements have not led to the full consolidation of national cybersecurity, to which Morocco is still exposed to cyber threats. National security is also in a critical situation due to the targets aimed at during the course of these international events. In addition to national security and stability, the fact that these criminal activities under study also affect economic integrity and the normal con-duct of financial and commercial transactions during these global events. Economic stability during these international sporting events will consequently be in question. This will consequently affect social stability and discourage efforts to strengthen national cybersecurity and the implementation of a specific resilience strategy.

### *2.1 Typology of Cyber Threats against Morocco*

In this paragraph, we attempt to establish a classification of the types of cyberattacks that Morocco faces on a permanent basis. This classification will take into account the nature of cyber-attacks, ranging from those aimed at individual gain to threats targeting objectives for political or ideological reasons.

First of all, cybercrime in its most widespread and low-intensity forms have seen an unimaginable rise in Morocco in recent years. The galloping rate of inter-net access in Morocco, accompanied by ignorance in cybersecurity and the illiteracy of the general public regarding computer security measures, has caused an unprecedented rise in online criminal activities. Identity theft, online fraud, financial scams, phishing, etc., are all the most common forms of cybercrime in Morocco. This cybercrime, according to Airaj (2024), experienced an explosion during the pandemic period, during which criminals took advantage of hyper-connectivity and individuals' uncontrolled access.

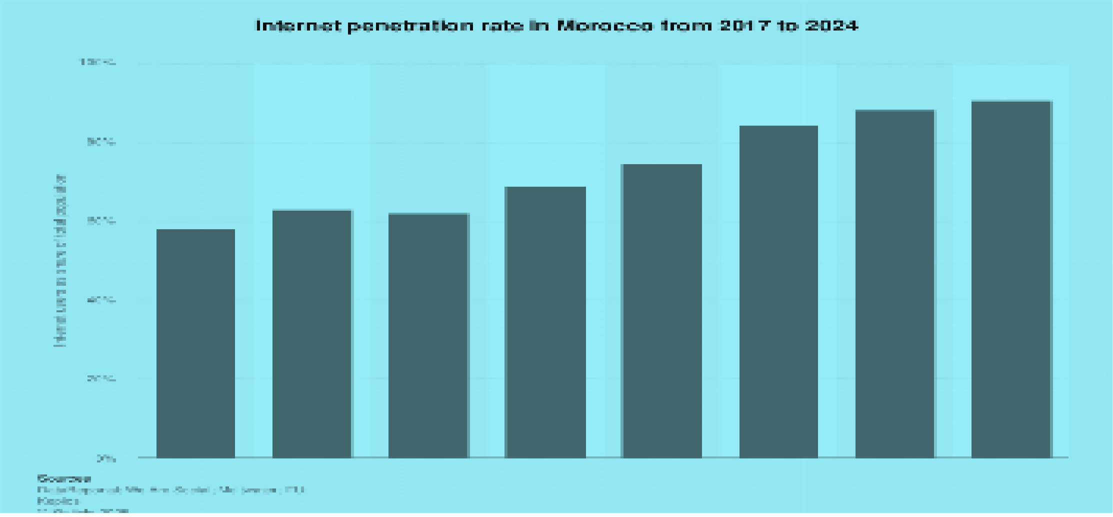

**Figure 1.** Demonstrate Internet penetration rate in Morocco from 2017 to 2024[1] .

Secondly, cyber espionage currently constitutes the most prevalent act in cyberspace due to the potentials it offers to instigators in terms of stealing sensitive data related to economic, military, and strategic matters, etc. Thanks to the potentials of anonymity and damage that this activity can inflict on adversaries with-out the slightest hesitation, actors of different natures, states or even non-state criminal actors, are interested in it and are racing against time to acquire its potentials not only at the global level. However, the North Africa and Middle East region has seen a rise in the use of these criminal methods in recent years[6].

In the third position, we see that the political reasons and ideological motives in the region are numerous due to regional geopolitical competition, causing local political movements to integrate into social destabilization strategies through cyberattacks. These social movements, in order to express their protests and refusals of policies, used computer devices to carry out attacks against government property, especially those that are online, to better convey their message to the public. These movements can target public websites, vital digital installations and infrastructures, or even critical digital platforms not only to disrupt their operations and services. However, to use them to spread their propaganda messages and psychological warfare through these online platforms.

Cyber-attacks targeting critical infrastructure, especially in Moroccan cities, pose a major security challenge. Moroccan cities are increasingly dependent on digital infrastructures providing vital services for citizens and urban logistics, specifically hospital, energy, and transportation services. In this regard, Choureik (2024) estimate that, the risks from cyber interventions targeting the vital infrastructures of Moroccan cities transitioning towards the digitalization of their infrastructures to become Smart cities, constitute the major challenge and the primary concern for Moroccan decision-makers, especially those targeting energy, health, and transportation infrastructure networks.

As we have highlighted in this paragraph, the political and ideological back-grounds provide the logical basis for reconstructing the criminal vision against Morocco's national security. Especially since the presence of multiple geopolitical and strategic motives and stakes in the region not only fuels interstate competition but also provides a pathway for instigators to exploit confrontations to achieve radical objectives. The methods of taking action to achieve such objectives can vary from propaganda, disinformation, social and political destabilization, to influencing public opinion, as previous experiences have shown us that these activities gain more prominence in vulnerable and densely populated regions[7].

### *2.2 Measure the extent of cyberattacks against national security*

Cyberattacks against critical infrastructure generally appear in scale and impact similar to cyberattacks targeting other states, especially those in the MENA region, which face several challenges questioning the level of national prepared-ness and cybersecurity. In this section, we observe that under certain conditions, the disruption can be doubled or even intensified, causing significant disturbances in vital services such as energy and hospital services, and finally in transportation logistics. We also add that the impact can only be complete and devastating with the achievement of other objectives, especially in the banking and financial sector, and if the cyberattacks have the assurance of financial resources and the necessary level of expertise, the damage to this essential service will be colossal [8].

It is obviously during the disruption of an essential digital financial or economic system that the damage and losses will be catastrophic, especially during the organization of an event with international significance. Economic activities, financial and commercial transactions, and all other activities attached to these targeted systems will suffer unavoidable losses and damages, as well as stoppages and disruptions in their services and activities if they are targeted by well-organized cyberattacks. The trust and reputation of national services in this area of economic value will be affected, causing individuals to lose confidence in the financial and banking transaction system due to cyberattacks targeting their accounts. So, if the projects and open works of smart cities in Morocco do not take into account the challenges of cyberattacks as Choureik (2024) confirm, against the overall security of Morocco, it will render inadequate the measures and efforts for acquiring resilient and in-depth cybersecurity.

Public trust eroded in banking and financial systems in the event of attacks or disruption is equal to public trust in national public order systems in the event of humiliation and disruption by cyberattacks. Trust is an essential element to consolidate, and successful cyberattacks against national institutions and establishments can provoke a wave of distrust regarding the capabilities of these national bodies to ensure national security. Because in the case of low trust in sensitive institutions and their ability to maintain national integrity, this can cause social unrest due to citizens' scepticism towards national agencies and their ability to establish public order.

Finally, the accumulation in the scale of cyber-attacks will lead us to identify riskier cyber threats, those of cyber terrorism and strategic cyber espionage. Although the first term is still anchored around its reality and effects, some activities have been detected against military installations, government infrastructures, and essential economic assets of certain countries, aiming to achieve large-scale objectives[9]. For this Youssef (2024) add, the Moroccan legislation remains, in this regard, somewhat timid but emphasizes the necessity of robust and solid measures against these criminal activities.

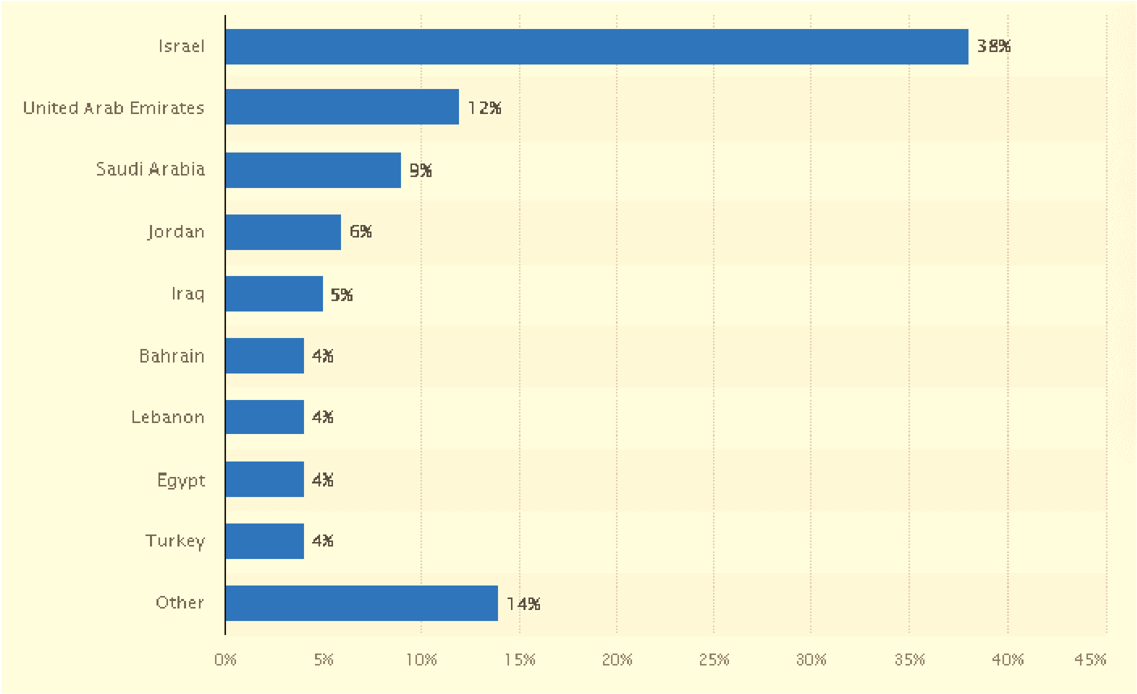

**Figure 2** Demonstrate Middle East and North African countries most targeted by nation-state or state-affiliated cyber threat actors from July 2022 to June 2023[2].

*2.3 Issues of inspection and recognition of cyber threats*

The problem of identifying cyber-attacks in cyberspace is a priority challenge for all countries, as criminals always take advantage of technological advancements and their criminal cunning to make their attacks discreet and unidentifiable. The challenge is therefore the same for Moroccan decision-makers who manoeuvre to make these processes identifiable and real so that the law can take its course in establishing order.

The cyber threat in Morocco, as in several other countries, takes advantage of the potentials of anonymity and discretion to stay far from judicial authorities. While criminals still remain in most cases, especially in cases where advanced computer capabilities, advanced computer equipment, and solid psychological and political backgrounds exist to commit the criminal acts. The problem of identification is more complex when attacks can be carried out outside national territories and involve obfuscation devices that complicate the processes of investigation and attribution of actions in cyberspace[10]. As Kenza debate (2024), the issue of identification is not only a matter of judicial investigations or legal procedures, but the technical aspect also constitutes a challenge for the accomplishment of the processes of identifying criminal acts in cyberspace. Although Morocco continues to make progress in the field of digitization and digitalization of activities and infrastructures, the lack of human resources and national technological expertise constitutes another serious challenge for Morocco to address. Morocco needs, to consolidate its efforts in governance and national law in cyberspace, a well-advanced national professional elite in research and qualified in computer development. The positioning of technical capabilities in the process of strengthening institutional efforts is essential, even necessary, in order to establish a real and solid cyber defense.

In this sense, Elder (2020) continue the debate by confirming, the fact that the cyber threat surpasses the territorial and border aspects in terms of effects includes the necessity to provide broader frameworks of collaboration in the hands of Moroccan decision-makers so that they can overcome critical situations. It is in this sense that international cooperation with various actors, not only state actors, who are interested in the challenges and issues of cyberspace, should be diversified and strengthened by the Moroccan state in order to improve Moroccan expertise and professionalism in cybersecurity and cyber governance, as well as to consolidate collaboration in intelligence matters and the deep fight against cybercrime.

In addition to the transnational nature of the cyber threat, the evolving aspect of the cyber threat questions the efforts of professionals at the international level, as they base their responses on rigid and non-evolving practices. The absence of adaptation at the level of frameworks with criminal innovation implies the necessity of innovation at the level of practice and the production of internal legal and institutional frameworks. The necessity of having an innovative internal policy on cybersecurity that takes into account criminal advancements is a logical step to reduce the adverse effects of complex cyberattacks[11].

The Moroccan security environment risks being threatened by cyber challenges not only after accepting the challenges of organizing international events. However, the cyber threat has been making its presence felt against official and individual activities for some time now. In this sense, this ever-present cyber threat risks permanently undermining economic growth, social stability, and the security of national territories. And despite the numerous efforts by Moroccan authorities to consolidate the frameworks of cyber governance and cybersecurity, the needs for resources and international collaboration continue to weigh against national efforts to balance the situation. That is why, in this chapter, we attempt to pre-sent the main ideas to overcome this critical situation by introducing an innovative and multifaceted approach in partnership, collaboration, and investment, etc., which covers all areas already in critical condition and in need of cyber resilience.

## 3. The Needs of Cyber Intelligence for National Security

### *3.1 What cyber intelligence means and why it is important?*

Intelligence generally refers to the collection of data, analysis, and finally the interpretation of the information collected according to the situation. So, intelligence in cyberspace or cyber intelligence refers to the same applications of gene-ral intelligence, with the specificity of the operational fields being the basis for the difference, while it still maintains the same objectives of anticipating and mitigating such threats, ensuring stability, and preserving national security[12]. The role of intelligence in cyberspace is extremely important compared to traditional intelligence due to the necessity of monitoring information in the new fields of competition and geopolitical rivalry. Moreover, cyber intelligence provides decision-makers with a comprehensive view of the situation within cyberspace and how trends, ideas, and debates evolve, as well as gaining experience on the innovations in the criminal use of technological devices and how criminals can exploit them to achieve objectives that undermine national security and stability. In this sense, cyber intelligence or intelligence in cyberspace provides more advantages to traditional or classic intelligence activities by integrating new technological devices for the collection and analysis of sensitive data such as the potentials of artificial intelligence and also the detection of predicted threats [13].

The process of digitizing key activities such as energy supply, digitalization of hospitalization, organization and management of urban traffic and logistics transport, to which the growing digital management of Moroccan cities not only increases the need for strengthening national security within these urban spaces due to infiltration and hacking issues, etc. However, this reinforces according to Choureik (2024), the need for security measures in cyberspace and also the possibilities of extending intelligence activities within cyberspace in order to stabilize the situation and at the same time limit the effects of harmful activities within and across cyberspace. The digitization projects that Morocco is undertaking parallel to the limits of security policies within cyberspace reflect the importance of such a robust strategy in cyber intelligence, to which the cyber threat, as we have demonstrated in the previous paragraphs, has become transformative and mutating, moving from the traditional position to new dimensions and devastating effects.

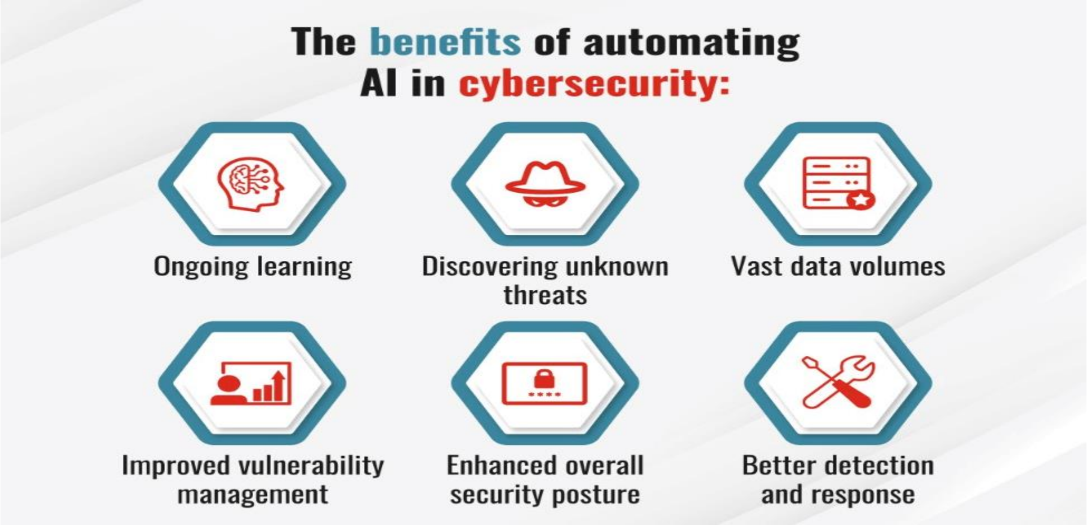
The benefits of automating AI in cybersecurity:
Ongoing learning
Discovering unknown threats
Vast data volumes
Improved vulnerability management
Enhanced overall security posture
Better detection and response

**Figure 3** Benefits Of Artificial Intelligence (AI) In Managing Cyber Risks[3].

*3.2 Why we need the integration of cyber intelligence into the national security strategy*

We observe that the integration of cyber intelligence within the overall nation-al security strategy is a step forward for the consolidation of security practices and the application of the law within cyberspace, as well as an opportunity for the strengthening of cyber governance measures that Morocco has been committed to for years at both the national and international levels. Because the potential use of digital devices for data collection and analysis allows for better detection of threats within cyberspace and thus better deterrence and applicability of law and attribution of responsibilities instead of letting cybercriminals benefit from the potential for discretion, free from responsibilities and far from the frameworks of law and legislation[14]. The use of the potential of artificial intelligence for the analysis of collected data and traffic flows within the network improves the detection of cyber threats and also ensures more effective responses against predicted anomalies and violations[15]. The use of artificial intelligence for detecting cyber threats has become widespread among national security actors, and security agencies have been using it to improve their resilience levels against the ever-evolving cybercrime. For example, China uses the potential of artificial intelligence to detect anomalies and online threats and also to enhance cyber defense deterrence[16]. The United States also uses these potentials to counter cyber threats, especially those of cyber espionage and theft of defense secrets and ransomware against the country's critical infrastructure. Several other states and security agencies are taking advantage of these potentials and engaging in similar processes to improve their rates of combating cyber threats using the potentials of artificial intelligence, which statistics show can reduce the detection of cyber-attacks by 95% [17].

The benefits of cyber intelligence are numerous as we can use the potential of computer systems to enhance activities of collection, analysis, and detection. This helps us minimize the detection and response time by reducing the duration between identifying the threat and responding to its effects on one hand. On the other hand, the automated response by the systems used also seems effective in the absence of personnel and agents in the field to deter such criminal activity. Proactivity and the superiority of these activities offer us against the transformation of threats in cyberspace, as Choureik (2024) add, the stability and security during the organization of such international events, which is important, even crucial, in order to improve the protection of critical infrastructures and ensure the stability of vital services during a global occasion. We know that in Morocco, cybersecurity remains selective for multiple reasons and varies according to the priorities of the sectors and areas under protection according to Kezzoute (2024). In this sense, we believe the conclusions of Airaj (2024), when he said that cyber intelligence and cybernetic intelligence can fill the gaps in our national cyber strategy by providing a sense of security and stability, even trust, and also by offering support and investigative assistance to institutions and organizations dedicated to law enforcement, instead of leaving the field open and free for criminals and their harmful activities.

It is in this aspect that we can observe that the role is far from merely taking advantage of the potential of technological devices to improve national cybersecurity. But in the contrary, Trim and Lee (2025), sees that the introduction of cyber intelligence also promotes cooperation and collaboration among public national institutions to fill the gaps, giving rise to an institutional network of collective cyber defense and cybersecurity against cyber threats. They continue to says, that the sharing of information's between national agencies dedicated to national security and defense and private entities also allows, in the process of collaboration and cooperation among the nation's actors, to improve the vision of the national cyber strategy. This interaction between intelligence entities, national security agencies, and judicial, governance, and law enforcement institutions, etc., often implemented in several countries, allows, in the presence of inter-governmental coordination, to strengthen the national security and strategy of these countries to counter the transformation of cyber threats.

### *3.3 Case study demonstrating the efficiency of cyber intelligence in preventing cyber threats*

As we have seen, several states are currently adopting cyber intelligence pro-cesses and extending their intelligence activities within cyberspace.  National security at the international level is currently under threat from various activities in the cyber world, just like in the real world. Cyber-attacks, mutated thanks to techno-logical advances, have helped criminals within the network to develop their activities and achieve greater impact, giving their actions more scope by surpassing the simple goals of personal gain or moral satisfaction to more devastating acts against vital state interests and objectives[18]. Ransomware at-tacks, for example, have evolved from targeting individuals to manipulate their personal identities or steal their banking data, to attacking critical infrastructures, such as the ransomware cyberattacks against critical energy infrastructures that successfully took hostage the sensitive data of the Colonial Pipeline company in the United States, for instance. However, Kolade (2025) add, that the adoption of a prevention strategy based on intelligence and assisted by the adoption of the potentials of artificial intelligence to prevent cyberattacks has helped the company avoid negative and largescale impacts. Intelligent analysis using advanced artificial intelligence capabilities to detect vulnerabilities in the company's computer systems has improved the detection and prediction rate to 95%. The case of the American company highlights that the adoption of technological advancements, especially those in artificial intelligence, to improve cyber intelligence constitutes the best choice to consolidate the vision for a specific national cybersecurity strategy, strong in detection and response against large-scale cyberattacks on national critical infrastructures.

The second example is India, in the same area of combating cybercrime, but this time intelligent detection is dedicated to phishing and the theft of sensitive data in the financial sector. The fact that India is dedicating more efforts to developing the electronic financial sector poses several problems of financial cyber-crime for it. The theft of monetary data, targeted financial transactions, identity manipulation, online fraud, and money laundering, etc., constitute the types of cybercrime for which AI-based cybersecurity solutions in India have been mobilized to detect and reduce financial risks preventively [19].  The national security and intelligence agencies in India have undertaken specific processes of artificial intelligence model learning, which have enabled these systems to automatically detect potential risks on networks and send alerts to agents and decision-makers regarding detected critical situations[20]. This practice reinforces, according to our trajectory of analysis and argumentation, the justification of the importance of adopting artificial intelligence in national security issues.

In this regard, the integration of cyber intelligence, drawing on previous experiences, constitutes an opportunity for Morocco that should not be overlooked in terms of the potential that cyber intelligence offers for national security and stability. Because of the large-scale social and economic impact digital initiatives and projects that Morocco is undertaking, alongside the presence of multiple vulnerabilities that we are still far from covering, decision-makers, including supervisory authorities, will find themselves in a critical situation. That is why we are engaged in an analysis process as the same Choureik analysis (2024), indicating the importance of cyber intelligence and its relevance for Morocco in order to overcome the vulnerable situation and mitigate the risks arising from massive digitization in Morocco. In parallel with this diagnosis, we believe that the consolidation of other programs and planning can constitute a strong point in the process of achieving the national cyber strategy in cyberspace and national security. In this context, strengthening awareness frameworks and developing digital consciousness, as well as consolidating ethical frameworks, including interpectoral collaboration and among multiple and diverse actors, all constitute the cornerstone in the process of consolidating passive practices in cyberspace.

We are consolidating the argument around the relevance of cyber intelligence practices and the necessity of its existence within a national security strategy as a preventive response to ever-evolving cyber threats that pose a danger to Morocco's vital infrastructures. Because the extension of intelligence activities in cyberspace and the parallel use of technological devices to improve the existence of these services and organizations in cyberspace constitutes a step forward in the process of strengthening national security on one hand. On the other hand, the activities of resource and time optimization, threat detection, big data analysis, and automated responses by the adopted systems reflect the necessity of adopting these devices to ensure resilience and deterrence in Moroccan cyber territories.

## 4. How to Ensure Effective Strategic Management against Cyber Threats?

### *4.1 Requirements for a robust national cyber strategy*

Filling the gap in the national cyber strategy around the aspects we discussed in our article is essential to ensure solid and effective protection of vital infrastructures and sensitive data at risk. To consolidate the strategic vision of Moroccan decision-makers around the evolving challenges and issues in cyberspace, the integration of concise evaluation processes, the consolidation of protection and response measures and procedures, and the strengthening of cooperative and collaborative frameworks are the main points to achieve a strategic vision that takes into account the changing nature of threats in cyberspace[21].

For further clarity, the process of identifying online risks requires an in-depth evaluation through the use of specific technological devices that will not only help facilitate the online detection of potential risks. But, it also contributes to reducing costs and optimizing human and financial resources [22]. Privacy issues also should be addressed in parallel with national security concerns and the priorities of social stability. For this reason, Qudus (2025) add, in order not to let cyber intelligence measures and a purely security-oriented vision negatively impact ethical considerations and freedoms in cyberspace, that a comprehensive strategy aimed at deterring evolving cyber threats should highlight these considerations of respecting privacy and personal data requirements.

In addition to the above, the strategy under discussion should include well-explained automated response protocols to ensure the effectiveness of these pro-cesses and stealthy mitigation against cyber threats, reducing impact and scope preventively. In this aspect, these protocols should clarify the modalities of use and the types of interventions to avoid the misuse of automated responses and prevent unforeseen violations [23]. The fact that cyber threats are mutating and transformative, they are also transnational.

To this end, this study unlike consider that cooperation and collaboration are crucial elements for mitigating the objectives of national cybersecurity. We observe that in this cooperative aspect, the sharing of information between agencies and supervisory institutions contributes to the creation of a coordinated national cybersecurity and cyber defense network. The stakes and challenges in cyberspace are numerous, making it not just a space of competition. However, a space of manipulation and instigation in which cyber threats can take other forms and magnitudes that we believe and know. For this, the presence of an open, dynamic, adaptive strategy is a step forward in preparing nations against this threat-ening situation[23].

### *4.2 The consolidation of diversified intergovernmental and intersectoral collaborative relationships*

The fact that the cyber threat is transnational makes the efforts to counter this threat a shared responsibility among several actors. From this situation, Morocco's 2030 cyber strategy emphasizes the collaborative aspect, but according to a paradigm, in other words, a classical or traditional one. The actors recommended to collaborate with the Moroccan State to mitigate potential risks in cyberspace in normal situations are only the official actors in international life[24]. While we emphasize in our analysis that diversifying partner-ships and collaborations to ensure the effectiveness of such a cyber-strategy against cyber threats directing their potential attacks towards the country's critical infrastructures, by leveraging the experiences of the relevant actors, can help Moroccan decision-makers improve their visions and strategic planning in cyberspace. Technology firms, security agencies, international entities, and all other institutions dedicated to the development of policies, planning, and cyber strategies or risk management should be called upon to contribute to the implementation of the national plan and to refine the national cyber strategy, which is still vulnerable to the changes we detected during our analytical process, as Tim and Lee (2025) debates.

Diverse partnerships, especially those with the private sector due to its experience in the field of cybersecurity, strengthen the potentials of cyber intelligence. On one hand, by sharing experience reports on potential attacks and assessments of the potential impacts and scales of cyberattacks with cyber intelligence services that wish to engage in cyberspace. And on the other hand, by providing these organizations with the necessary tools to carry out their tasks effectively[25]. However, the framework of diversified partnerships we need to establish these collaborations, based on multiple international initiatives among different actors that blur the lines between the nature of official actors and those of the private sector, still requires more clarity around aspects of transparency and trust.

For this, these frameworks require a concise commitment to the development of specific regulatory frameworks, facilitating and organizing the sharing of in-formation between national and international organizations of diverse nature. Far from improving regulatory frameworks, these commitments also enhance the global posture in terms of cybersecurity and the mitigation of the evolving cyber threat [26]. States at the international level, despite maneuvering against cyber challenges and digital issues according to the legacy of the international system and institutional and organizational accumulations. States maintain their maneuvering spaces, free from international constraints, and try to consolidate their cooperative efforts with international actors.

But, who are not members of the international community as we have listed as the non-states actors. This kind of partnership and collaboration can improves as Obioha (2025) defend, the level of resilience of states in the field of cybersecurity, by giving states, through the sharing of essential information in the security domain, the upper hand in the fight against cyber-attacks, especially against cyber espionage and ransomware. Also according to Sadhia (2024) reflexions, the national cyber strategy and the strategic vision of the Moroccan national supervisory authorities, in effect, through the adoption of partnerships according to this innovative framework, may overcome its state of deficiency regarding this situation and evolve its cybersecurity processes to deter the complex and ever-evolving cyber threat.

### *4.3 Develop professional capacities and the training offer in cyber-security*

According to Kolade (2025), the development and investment in national cybersecurity potentials are not limited to cooperative aspects or the encouragement of adopting technological processes for intelligence services in order to strengthen national resilience against potential cybersecurity risks. However, the need for human resources and personnel proficient in the recommended systems requires decision-makers and supervisory authorities to direct a portion of the national effort towards the development of these sectors, where training and the development of professional offerings in the cyber domain also constitute the cornerstone of this targeted strategy. For example, artificial intelligence technologies in analysis, detection, and replication, as well as the processes of training and learning these artificial intelligence systems, all require a certain level of professionalism and technical expertise, given their primacy in current security matters[26].

Given that these tools have demonstrated their effectiveness on several occasions and examples, the need for professional expertise and technical qualification at the national level to master these tools and their potential in favor of national security remains a challenge to achieve the objectives of national cyber-security[27].

In this regard, the promotion of education and professional qualification programs within training institutions and education at all levels is essential to equip professionals, executives, technicians, developers, and analysts in order to mitigate security and stability objectives[28]. In parallel with the incentives to channel investments towards the training of executives and experts in the field of cybersecurity and the development of IT professionals. The development of national digital infrastructures, so that they adapt to the capabilities of new security technologies embedded within our digital infrastructures, and which consume large amounts of energy and connectivity while also degrading the environment, is also a necessity alongside the development of areas that strengthen national resilience in cyberspace[29].

At the same time, and related to Patil (2025) conclusions, we encourage decision-makers to also develop specific pro-grams to promote innovation in cybersecurity based on advanced technologies in quantum encryption and AI-based cyber defense, for example, in order to out-smart criminal ingenuity in technical terms and anticipate their recourse and criminal tactics against the country's critical infrastructures. The Moroccan government should, in order to secure national cyber territories against evolving cyber threats targeting critical infrastructures and national assets during the organization of an event with international connotation, ensure the necessary re-sources and the required professional, financial, and technological capacities to guarantee a stable, adaptive, and resilient system[30].

## 5. Recommendations for Well-Functioning of Cyber Intelligence in Morocco

To overcome the critical situation, we discussed in our article, Morocco should develop its cyber strategy according to the requirements of criminal cunning, where technological advancements, political instigation, and ideological confrontation can serve the objectives of destabilization and weakening of the political and social order during the organization of an event with universal connotations. We recommend in this section the strengthening of the legal framework, ensuring the necessary funding for the development of such initiatives and innovations related to cyber intelligence or cyber intelligence and all other plans attached to these proposals. The position of the individual is always concerning in online destabilization strategies, which is why we acknowledge the need for raising aware-ness and developing individuals' consciousness and knowledge about what the ever-evolving cybercrime imposes on national security and stability. The consolidation of public education programs at all levels of teaching, as well as outside known institutions, constitutes the cornerstone in the willingness to act preventively against these security threats and dangers. This will also help us build solid and resilient infrastructures capable of maintaining service continuity away from interruptions caused by online criminals.

### *5.1 Revitalization of the current legal and regulatory framework*

According to Abbadi (2025), Morocco's strategic vision for cyberspace in 2030 is no longer aligned with the ambitions of the national professional elite in cyber-security, with legal and cooperation gaps being at the forefront of its shortcomings. Due to these obstacles and gaps in the legal frameworks, including reservations around the cooperative aspect, Morocco cannot accelerate the implementation of regulations nor effectively deter cybercrime. For this reason, the presence of legal frameworks adapted to new developments and capable of addressing the challenges of online crime, as well as being proficient in capturing the related changes in this crime in cyberspace in cognitive and technical matters, is essential to ensure the stability of international events organized in Morocco.

In this regard, we recommend that updates to the legal framework should take into account the libertarian requirements and individual rights, as prioritizing security demands over respect for local and societal specificities hinders the application of the law if Moroccan decision-makers ignore these particularities. The proposals should also be aligned with the requirements of international standards in the field, especially in cybercrime, cybersecurity, and cyber governance. Harmonization of legislation concerning the standards of cyber intelligence with new criminal developments by granting more prerogatives to the relevant agencies to prosecute criminals through articles or codes related to cases and types of cyberattacks. In this process, we see that law enforcement should also take the pursuit and arrest of criminals more seriously, for which Morocco is supposed to strengthen cooperation and provide the legal basis to genuinely deter the evolving online cybercrime and legitimize actions against this cybercrime[31]. Finally, we see in the aspect of legal and regulatory mechanisms that strengthening the roles of law enforcement instruments is also essential to ensure the effectiveness of law enforcement, including the consolidation of legal standards and ensuring a stable and safer digital environment.

### *5.2 Generously ensure the necessary funding for the implementation of cyber intelligence in Morocco*

Generous funding offers more advantages for the development of security capacities and skills. Ensuring the necessary funding for a better implementation of cyber intelligence in Morocco will help Moroccan decision-makers recruit more professionals and talents in cybersecurity at the international level from all sectors. Additionally, the existence of financial resources, can help improve specialized institutions by aiding these establishments in regenerating and renewing themselves in terms of equipment, human resources, and work-related infrastructure and logistics. In the same vein, we believe as Abbadi (2025), that this will support the country's positioning regarding the possession of technologies, through the purchase and acquisition of advanced cyber threat detection technologies.

The presence of necessary funding can also serve as a basis to revive national investments in areas helping national authorities secure blockchain transactions, harness the potential of artificial intelligence in security detection and analysis, develop cloud technologies, etc. this will undoubtedly help the Moroccan authorities to effectively combat evolving and sophisticated cyber threats. The diversification of partnerships, as we have outlined, will help decision-makers diversify their sources of funding while private sector actors can provide crucial funding to develop programs addressing cybersecurity issues, which we are tackling within cooperative frameworks[32]. Indeed, the presence of necessary funding for the development of innovation processes and the upgrading of Morocco's digital infrastructure is essential to promote the development of effective solutions and response strategies tailored to the specificities of the threat and Morocco.

### *5.3 Strengthening public awareness*

Although the Moroccan State will provide the necessary capacities and re-sources in funding and supply, the training of individuals remains an essential point to avoid losses due to human ignorance. We have noticed that raising awareness and training the general public is a fundamental element in Morocco's national cyber strategy for 2030[33]. However, awareness programs should be strengthened and also diversified and shared with all levels of education and training and with all social categories. Alongside public programs, the Moroccan state should also provide specific programs for specific entities, especially small and medium-sized enterprises, government agencies, including institutions operating in the civil sector, should all be targeted by these awareness programs to mitigate national cybersecurity objectives and reduce the impacts and scope of cyber risks.

This will help the supervisory authorities benefit from a culture of good practices rooted in society and based on the ethical use of cyberspace, which will be embedded within society and will directly lead to the reduction of criminal intentions and malicious thoughts, and consequently the rate of internal crime in cyberspace. The awareness component is ubiquitous in most international cyber strategies, and experiences in most states demonstrate that these programs combating digital and technological literacy have a very positive impact on reducing the rate of cybercrime and promoting cybersecurity and stability in cyberspace[34]. This will not only impact crime rates but also promote social stability and security. However, supporting the existence of these programs within such a society transforms that society and makes it sustainable and resilient in the face of the changes in cybercrime.

Our recommendations constitute a roadmap for an urgent call for the introduction and adoption of cyber intelligence and intelligence within cyberspace in order to avoid the dangerous impact and extent of mutant cybercrime against infrastructure and vital assets during a globally significant sporting event in Morocco. We should, to achieve this objective, ensure the commitment and obligation of the entire Moroccan community, from high authorities to ordinary citizens. The allocation and assurance of resources, as well as the reduction of bureaucratic constraints that can constitute obstacles to the implementation of solutions against cyber threats, is an important step in this process. To ensure the achievement of the planned objectives, the presence of a complementary strategy or a specific cyber strategy, etc., regardless of the name, is important to guarantee digital security and the resilience of vital digital infrastructures in Morocco.

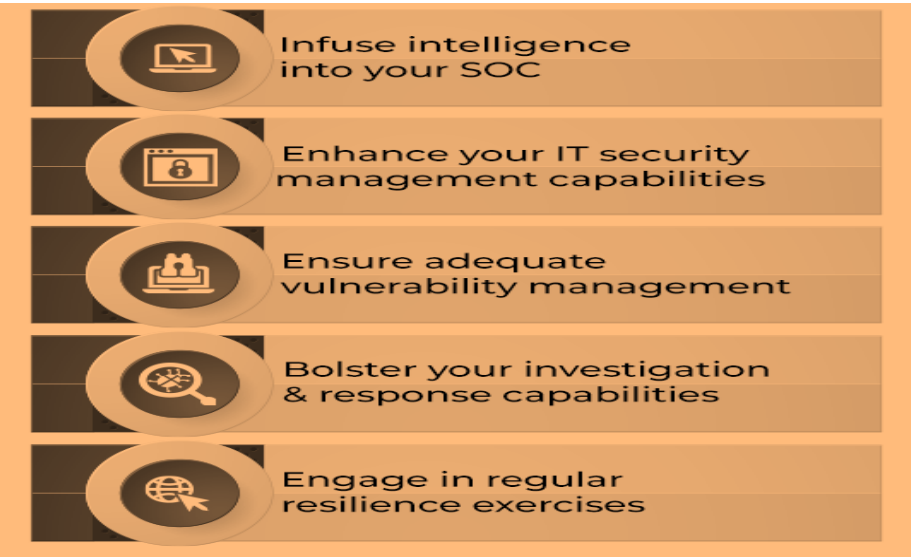
Infuse intelligence into your SOC
Enhance your IT security management capabilities
Ensure adequate vulnerability management
Bolster your investigation & response capabilities
Engage in regular resilience exercises

**Figure 4.** Best Practices for Cyber Intelligence Threat Management[4].

## 6. Conclusion

Before presenting the conclusion of our work, we want to summarize the main ideas we have gathered on cyber intelligence and national security in Morocco. In our article, we addressed the crucial role of cyber intelligence in consolidating national security measures and social stability. We also prioritized Morocco as a case study during this research by analysing its level of resilience and cybersecurity-ty and exploring ways to improve the country's cyber capabilities in cybersecurity. We found that Morocco has indeed accumulated a significant level in the development of digital infrastructures and in the development of the national cyber strategy standards. However, we have observed that several challenges and issues still persist, especially regarding legal and regulatory standards. We also noted that funding is also insufficient and that it is exacerbated by the lack of perfect public awareness around the challenges and issues under discussion. The cases we introduced during our study provided us with valuable knowledge about the potential advantages for improving national security and stability. And in this aspect, we applied this perspective to the Moroccan context, giving rise to a robust approach that ensures cybersecurity in the face of the rise of mutating and trans-formative cyber threats. In this section, we found that the presence of a national strategy integrating innovative national policies in terms of international collaboration and processes for acquiring technological advancements is essential.

The research recommended complementing the national cyber strategy for 2030 and the national public policy on cybersecurity. This reformulation that we recommend should adapt to regulatory needs and transform response frameworks to address new challenges in cyberspace. In this sense, we have also recommended the respect of libertarian principles and individual rights when implementing such integration of intelligence in cyberspace to strengthen national security. Innovative collaboration has also taken a primary position in our analyses, in which the necessity to extend collaboration with other actors in cyberspace, especially the private sector and international partners of various natures, constitutes the cornerstone for establishing a robust and efficient national cybersecurity. In addition to the above, Moroccan authorities should engage in specific and collaborative technological project initiatives to develop the level of cyber intelligence through the potentials of AI and to strengthen the country's capabilities against emerging cyber threats. Finally, public awareness proves to be paramount according to our analytical process, where the multiplication of training and education programs to develop the skills of personnel and citizens is essential to mitigate the risks associated with ignorance and human error, which constitute the weak link in any national security strategy and also in cyberspace. To take action, we have recommended the implementation of a proactive and multifaceted strategy as imperative so that Morocco can move to the stage of effectively mitigating cyber threats. In this process, Morocco should ensure the necessary funding to strengthen the capacities of technological infrastructures and the national network so that they can fill the gaps of a technical and techno-logical nature related to the degradation of equipment and the gaps in the operating systems within our infrastructures. These resources should also be directed to-wards the training of professionals and experts in national cybersecurity, as well as the establishment of new institutions for cybersecurity within the national territory, and the updating of existing institutions and training centers for professionals and experts in national cybersecurity. This should also support efforts for the acquisition of cyber technologies and the promotion of national offerings in this area in order to avoid tying the country's fate in national cybersecurity to import markets already under geopolitical upheaval. The cooperative aspect should be maximized and benefit from the newly established relationships in this framework to exchange information and intelligence, and in other areas, benefit from the transfer of foreign knowledge and expertise in the field of cybersecurity.

According to the financial and cooperative aspects, culture also plays a crucial role in strengthening cybersecurity. The campaigns for education and the development of knowledge and public awareness around cyber challenges and issues, which should target all social categories and economic, political, civil, educational entities, etc., should achieve their goals of developing national and civic culture around these issues and adapting public behavior to the disruptions from cyberspace. Cybersecurity culture should strengthen the feelings of trust among individuals and society regarding national cybersecurity policies and strategies by rooting the best practices of accountability and trust. The involvement of multiple and diverse stakeholders in the processes of implementing and embedding a culture of cybersecurity will strengthen national preparedness against large-scale cyber challenges. These cross border and globalized cyber challenges should encourage Moroccan authorities to adopt a new paradigm of cooperation and collaboration based, in addition to sharing information and expertise, on the consolidation of intelligence roles in this new strategy by establishing common institutions between the concerned international and internal actors to strengthen intelligent cooperation and simultaneously enhance Morocco's presence in global organizations, international treaties, and various conventions related to the cybersecurity aspect. Engaging in a globalized approach will, in our view, help Morocco achieve its objectives of consolidating national cybersecurity efforts and also strengthening the roles of national intelligence in national cyber territories.

We have developed enough recommendations around the discussed topic. However, we find that we still need more efforts to develop additional recommendations to effectively mitigate emerging cyber threats. In this section, we see that alongside the so-called main recommendations, the presence of a specific policy aimed at establishing a balance between cybersecurity needs and addressing gaps in related areas with legal and freedom issues can pose challenges to the implementation of the policies and recommendations provided, especially in the ignorance of these fundamental frameworks. More than the necessity to rethink the balance between security and freedom in the Moroccan context, the Moroccan state is supposed to invest in innovative solutions by introducing technological potentials and advancements in this field to strengthen national cybersecurity. In this sense, investing in the potential of artificial intelligence in cybersecurity and cyber defense, and the application of quantum computing to strengthen national cybersecurity, will be effective and operational solutions to enhance the applications of intelligence in cyberspace. To ensure the implementation of these recommendations, we see the creation of an institutional framework to coordinate these interinstitutional tasks, monitor, and also review the execution of the recommended policies.

The implementation of these policies will not only strengthen Morocco's national cybersecurity but also enhance intelligence and reconnaissance activities in cyberspace. However, this will improve Morocco's positioning in international cybersecurity rankings, and give Morocco the priority to establish itself as a regional leader in cybersecurity and related challenges and issues. Indeed, this demonstrates that intelligence and information gathering must be part of broader strategies and not just the national cybersecurity strategy, which, through the application of this vision, will succeed in building an effective ecosystem capable of resisting evolving and transformative cyber threats.

### Corresponding author

**Kezzoute Mhammed**
m.kezzoute@ump.ac.ma

### Acknowledgements

This article is produced through the unique efforts of the author and has received no external funding. This article used AI to rephrase sentence styles, correct spelling, correct grammar, generate citations, and correct style errors in the paragraphs. Finally, the article also contains data taken directly from their online sources.

### Funding

No funding.

### Contributions

K.M; Conceptualization, K.M; Investigation, K.M; Writing (Original Draft), K.M; Writing (Review and Editing) Supervision, K.M; Project Administration.

### Ethics declarations

This article does not contain any studies with human participants or animals performed by any of the authors.

### Consent for publication

Not applicable.

### Competing interests

All authors declare no competing interests.

## References

[1] Chouraik, C., El-Founir, R., & Taybi, K. (2024). Cyber-securing Morocco's smart cities: A case review. International Journal of Science and Research Archive. 13(01) 102–112. https://doi.org/10.30574/ijsra.2024.13.1.1619

[2] Airaj, S. (2024). The increase of cybercrime amidst the COVID-19 pandemic: A spotlight on the Moroccan context. Quantum Journal of Social Sciences and Humanities, 5(2) 204-212. https://doi.org/10.55197/qjssh.v5i2.388

[3] Youssef, E. H. (2024). The crime of "electronic terrorism" and the role of the Moroccan legislator in addressing it. Arid International Journal of Comminication & Information Sciences. 5(9) 6-31. https://doi.org/10.36772/arid.aijmscs.2024.591

[4] Security Conclave. (2024). Cybersecurity discussions on critical infrastructure and countering cyber criminality. https://securityconclave.com/

[5] Kezzoute, M.,(2024). The Geopolitics of Cyberspace: Issues & Challenges for Morocco by 2050. Thesis in Public Law, Mohammed Premiere University, Faculty of Law, Economy and Social Sciences, 286 pp.

[6] Perl, R., & Malisevic, N. (n.d.). A Comprehensive approach to cyber security – trends, challenges and the way forward. In A Comprehensive Approach to Cyber Security (pp. 47–49). https://connections-qj.org/system/files/ctwg_04_cybersecurity.pdf

[7] Elder, R.J. (2020). Cyberwarfare as Realized Conflict. In: Holt, T., Bossler, A. (eds) The Palgrave Handbook of International Cybercrime and Cyberdeviance. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-319-78440-3_64

[8] Kenza, R., Zakia, E., Rajaa, R., et al. (2024). Cybersecurity and the automo-tive supply chain in Morocco: An exploratory study. European Journal of Eco-nomic and Financial Research. 8(4). 224-236. http://dx.doi.org/10.46827/ejefr.v8i4.1790

[9] Lewis, J. (Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. Center for Strategic and International Studies. 13 p.

[10] Kumar, R,. The Problem of Attribution in Cyber Security. International Journal of Computer Applications. 131 (7) 34-36. http://dx.doi.org/10.5120/ijca2015907386

[11] Yacob, M. N., Idrus, S. Idris, L. (2023). Managing Cybersecurity Risks in Emerging Technologies. International Journal of Business and Technopreneurship. 13(3). http://dx.doi.org/10.58915/ijbt.v13i3.297

[12] Trim, P. R. J. & Lee, Y. I. (2025). Cyber Security Management and Strategic Intelligence. Taylors & Francis Group.

[13] Kolade, T. M., Obioha-Val, O., & Balogun, A. Y. (2025). AI-Driven Open Source Intelligence in Cyber Defense: A Double-edged Sword for National Securi-ty. Asian Journal of Research in Computer Science. 18 (1) 133-153. http://dx.doi.org/10.9734/ajrcos/2025/v18i1554

[14] Kezzoute, M., (2025). Cyber Governance in Morocco: Between the Consolida-tion of Interne Status and the Enhancement of Global Positioning. Journal of Cy-berspace Studies, 9(1) 223-242. http://dx.doi.org/10.22059/jcss.2025.385012.1114

[15] Patil, D. (2025). Artificial Intelligence in Cybersecurity: Enhancing Threat De-tection and Prevention Mechanisms through Machine Learning and Data Analyt-ics. https://www.researchgate.net/publication/385881488_Artificial_intelligence_in_cybersecurity_Enhancing_threat_detection_and_prevention_mechanisms_through_machine_learning_and_data_analytics

[16] Zang,. F. (2020, September 23). China’s military employment of artificial intel-ligence and its security implications. The International Affairs Review. https://www.iar-gwu.org/print-archive/blog-post-title-four-xgtap

[17] Homeland Security. (n.d.). U.S. Department of Homeland Security Using AI to secure the homeland. https://www.dhs.gov/ai/using-ai-to-secure-the-homeland

[18] Ruhl, Ch,. Hollis, D. & Maurer, T. (2020). Cyberspace and Geopolitics: As-sessing Global Cybersecurity Norm Processes at a Crossroads. Carnegy Endowen-ment. https://carnegieendowment.org/research/2020/02/ cyberspace-and-geopolitics-assessing-global-cybersecurity-norm-processes-at-a-crossroads?lang=en

[19] Sowmya, N. (2024). A Study on the Role of Artificial Intelligence in Detecting and Preventing Cyber Crimes in India. International Journal of Advanced Re-search in Science, Communication, and Technology. http://dx.doi.org/10.48175/IJARSCT-22635

[20] Strengthening National Cybersecurity of India with the Use of Artificial Intelli-gence – CENJOWS. (2024, July 9). https://cenjows.in/strengthening-national-cybersecurity-of-india-with-the-use-of-artificial-intelligence/

[21] Qudus, L. (2025). Cybersecurity Governance: Strengthening Policy Frame-works to Address Global Cybercrime and Data Privacy Challenges. International Journal of Science and Research Archive. 14(1) 1146-1163. https://doi.org/10.30574/ijsra.2025.14.1.0225

[22] Hurzhii, S. (2024). Features of Ensuring Cyber Resilience of National Infor-mation Resources, Communication and Technological Systems that Ensure the Functioning of Government Authorities under the Conditions of Martial Law. http://dx.doi.org/10.37750/2616-6798.2024.4(51).317993

[23] Eltaeib, T., Abuzneid, A., & Elleithy, K. (2024). Proposed Framework for a Comprehensive Cybersecurity Risk Management Strategy. http://dx.doi.org/10.1109/LISAT63094.2024.10808119

[23] Sandhia, G. K., Ranjani, M., & Nithiyanandam, N. (2024). Cybersecurity: The Part Played by Artificial Intelligence. In book: Analyzing Privacy and Security Difficulties in Social Media (pp.213-246). http://dx.doi.org/10.4018/979-8-3693-9491-5.ch010

[24] General Direction of the Security of Digital Systems. Morocan Cyber strategy 2030. https://www.dgssi.gov.ma/fr/publications/strategie-nationale-de-cybersecurite

[25] Security Conclave. (2024). Cybersecurity discussions on critical infrastructure and countering cyber criminality. https://securityconclave.com/

[26] Chang, L. & Coppel, N. (2020). Building Cyber Security Awareness in a Devel-oping Country: Lessons from Myanmar ? Journal of Computers & Security 97(2) 101959. http://dx.doi.org/10.1016/j.cose.2020.101959

[26] Uzoka, A., Cadet, E., & Ojukwu, P. U. (2024). Applying Artificial Intelligence in Cybersecurity to Enhance Threat Detection, Response, and Risk Management. Computer Science & IT Research Journal. 5(10) 2511-2538. https://doi.org/10.51594/csitrj.v5i10.1677

[27] Admas, W., Munaya, Y., & Diro, A. (2024). Cyber security: State of the art, challenges and future directions. Cyber Security and Applications. 2, 100031. https://doi.org/10.1016/j.csa.2023.100031

[28] Nyame, L., Marfo-Ahenkorah, E., & Abrahams, A. (2024). Rise in Cyber Threats in the United States and the Need for Advanced Cyber Risk Mitigation Tools and Adequate Skills to Combat Cyber Threats. 1-11. https://www.preprints.org/manuscript/202409.1813/v1

[29] Goswani, S., Mondal, S., Ashish, J,. Cyber Security and Digital Economy: Op-portunities, Growth and Challenges. Journal of Technology Innovations and En-ergy. 3(2) 1-21. http://dx.doi.org/10.56556/jtie.v3i2.907

[30] Balisane, H., Egho-Promise, E., & Lyada, E. (2024). The Effectiveness of a Comprehensive Threat Mitigation Framework in NETWORKING: A Multi-Layered Approach to Cyber Security. International Research Journal of Comput-er Science. 11(06) 529-538. http://dx.doi.org/10.26562/irjcs.2024.v1106.03

[31] Abbadi, M. (2025). Cybersecurity Policy and Legal Challenges in Morocco: A Comparative Analysis. International Journal of Cyber Law, 12(1) 45-63. https://doi.org/10.54878/acgprq10

[32] Kuznetsov, O. Sernani, P., Romeo, L., Frontoni, E., & Mancini, A.(2025) On the Integration of Artificial Intelligence and Blockchain Technology: A Perspective About Security. IEEE Acess. http://dx.doi.org/10.1109/ACCESS.2023.3349019

[33] Ahn, K, T., (2024) The Human Factor in Cybersecurity: An Analysis of Emerg-ing Trends and Challenges. The 4th International Conference on Marketing in the Connected Age (mica-2024). https://www.researchgate.net/publication/384471305_The_Human_Factor_in_Cybersecurity_An_Analysis_of_Emerging_Trends_and_Challenges

[34] Abrahams, T, O. et al. Cybersecurity Awareness and Education Programs: a Review of Employee Engagement and Accountability. Computer Science & IT Research Journal. 5(1).100-119. http://dx.doi.org/10.51594/csitrj.v5i1.708