GLOBAL GOVERNANCE & SOVEREIGNTY FOUNDATION

Morocco Radar

KONRAD ADENAUER STIFTUNG Maroc - Mauritanie

Policy Brief °05

Cybersecurity in Morocco: From a wake-up call to a new era of digital sovereignty

GEOPOLITICAL MONITOR

While the Kingdom of Morocco has achieved significant strategic milestones in cybersecurity, a series of high-profile cyberattacks in 2024 and 2025 have exposed a critical vulnerability. The most notable of these was the April 2025 breach of the National Social Security Fund (CNSS), an event that serves as Morocco's definitive "Sputnik moment", a wake-up call that has compelled the nation to re-evaluate its digital defenses. This incident, occurring despite Morocco's Tier 1 ranking in the International Telecommunication Union's (ITU) 2024 Global Cybersecurity Index (GCI), highlights a critical gap between institutional readiness and operational resilience.
Historically, Morocco has invested heavily in cybersecurity infrastructure, allocating budgets under the 2012 National Cybersecurity Strategy and its 2024 updates. Yet, returns remain modest. Kaspersky reported 12.6 million web threats in 2024, ranking Morocco third in Africa. Examples include ransomware targeting car manufacturers in 2020 and the 2023 Medusa gang's leak from Bank of Africa (formerly BMCE), exposing client data across 18 African countries.

With the forthcoming hosting of the 2025 Africa Cup of Nations (AFCON) and the 2030 FIFA World Cup, Morocco has a unique opportunity to accelerate its digital ambitions. These global events position cybersecurity not merely as a defensive necessity but as a key driver of economic growth and digital sovereignty, providing a high-stakes platform to showcase a secure and technologically resilient nation. But it also puts Morocco in the spotlight of digital security, for visitors and its citizens.

Signals to Decode

The April 2025 cyberattack on the National Social Security Fund (CNSS) was a watershed moment for Moroccan cybersecurity. Described by some experts as the country's most significant cyber-attack to date, the incident exposed systemic vulnerabilities that undermined public and institutional trust. The scale of the breach was unprecedented, exposing the personal and financial data of nearly two million people from approximately 500,000 companies.

The attack revealed that even with a strong national strategy in place, a single, critical vulnerability could result in a devastating data exfiltration event. The CNSS incident, while not a classic ransomware attack, demonstrated the immense reputational and financial risk posed by a breakdown in digital defenses. In the aftermath, the CNSS launched a $4 million US Dollars tender to strengthen its security measures, a direct reaction to the severity of the breach.

This response is a clear manifestation of a reactive security posture. The national framework was in place, but the real-time operational response, particularly in terms of crisis management was lacking. The idea that Morocco's investments in cybersecurity have yielded "little return" is a misdiagnosis of the underlying issue. The problem is not a lack of investment at the national level, but a profound and pervasive lack of cybersecurity maturity at the institutional and corporate level. The CNSS breach is a painful illustration of this disconnect. The DGSSI has consistently provided an effective and serious policy framework since its inception, but the broader private ecosystem failed to comply with its recommendations. While the government has a robust, high-level strategy and is making significant investments, the widespread apathy among Moroccan businesses creates a fragile attack surface.

According to a SecureWeb report, 53 % of Moroccan businesses "do not care about cybersecurity" even after being informed of their vulnerabilities, and an astonishing 78 % only adopt a security strategy after experiencing a hack or breach. This widespread managerial negligence undermines national-level efforts. A large-scale government investment in national security infrastructure is diminished when a major institution or a critical sector is compromised due to a fundamental failure in governance and due care. The recent breach therefore demonstrates that the challenge is not a scarcity of resources, but a failure to cultivate a national culture of cybersecurity where accountability is a priority.

Does Morocco have a Role to Play?

Morocco's commitment to cybersecurity is institutionalized through the General Directorate of Information Systems Security (DGSSI).The DGSSI is the national authority responsible for developing and implementing the country's cybersecurity strategy. The recent appointment of Brigadier General Abdellah Boutrig as its new Director General by King Mohammed VI serves as a powerful signal of this strategic commitment:. The DGSSI's placement under the National Defense Administration and the appointment of a senior military official to its helm indicate that Morocco views cybersecurity as a matter of national defense and sovereignty, aligned with traditional military affairs. This strategic decision elevates the issue from a technical matter to a national security imperative. It is particularly critical since cybersecurity has increasingly acquired a martial dimension, exposing the nation to risks of sophisticated cyber conflicts and sabotage carried out by hostile foreign forces, which directly justifies the DGSSI's official attachment to the National Defense Administration. The DGSSI's mandate extends beyond technical security to include national coordination, capacity building, and the development of a legal and institutional framework for the entire country. [AM5]

As a key directorate within the DGSSI, maCERT (Moroccan Computer Emergency Response Team) serves as the national hub for monitoring, detecting, and responding to cyberattacks. MaCERT's services are both reactive and proactive. Its reactive services include managing incidents, providing alerts, and supporting responses to breaches. Its proactive services involve technological watch, security assessments, and the dissemination of security information. The effectiveness of maCERT's crucial work depends on the broader ecosystem's readiness to report and respond, highlighting the critical link between a central authority and the decentralized entities it is meant to protect.

Points of Vigilance

In response to the pervasive cybersecurity apathy in the private sector, Morocco is moving away from a purely awareness-based approach toward a new model of "carrot and stick" enforcement. The National Control Commission for the Protection of Personal Data (CNDP) is now issuing formal notices and is prepared to impose penalties on companies that fail to comply with Law 09.08 on data privacy . The legal framework includes significant fines, ranging from 1.000 Euros to 20.000 Euros, as well as potential imprisonment for offenses such as failing to implement required security measures or fraudulently collecting data. This new enforcement paradigm is a direct response to the private sector's reactive posture. The government is now using the "stick" of financial and legal penalties to force a behavioral change and ensure compliance, signaling a more serious and determined approach to national security.

Despite high level policy, the on- the -ground cybersecurity ecosystem remains vulnerable. There is a significant scarcity of specialized cybersecurity skills and financial constraints, particularly for Small and Medium-sized companies. Additionally, this is a culture where 40 % of businesses rely on a single IT

staff member to handle all security issues. A fundamental issue is that the human factor remains the most significant vulnerability in the cybersecurity chain. This is exacerbated by a pervasive lack of cybersecurity culture and a widespread vulnerability to social engineering attacks. Furthermore, there is a notable absence of a "secure by design" culture in software implementation, leaving critical systems with vulnerabilities that can be easily exploited.

OPPORTUNITIES & RISKS

Opportunities

Implement proven strategies

To move beyond a reactive posture, Morocco can look to the example of South Korea's proactive cyber defense strategy. This approach moves beyond simply responding to attacks to actively anticipating and neutralizing threats before they impact national infrastructure. This model is anchored in gathering intelligence on potential threats and collaborating with international partners to neutralize malicious attacks. South Korea's model provides an actionable framework that directly addresses the central problem identified in this brief: the gap between Morocco's strategic readiness and its operational resilience. Moving away from a purely reactive security posture and transforming a national vulnerability into a new resilient force.

Rise a homegrown startup ecosystem

Morocco's burgeoning startup scene presents a key opportunity to build a homegrown, agile, and innovative cybersecurity industry. The success of companies like Nucleon Security, which recently raised 3 million Euros in seed funding and formed a strategic partnership with Orange Morocco, demonstrates this potential. Moroccan startups can help address the national skills gap and provide tailored, cybersecurity-driven solutions to companies that traditionally lack the resources for robust security. The government's support through programs like 212Founders is instrumental in fostering these ventures and building digital sovereignty from within.

Network of International partnerships

International cooperation is a core pillar of Morocco's 2030 cybersecurity strategy. The nation is actively promoting partnerships to strengthen its digital defenses and share threat intelligence, essential given the transnational nature of cyber threats. A significant step was the Memorandum of Understanding (MoU) signed with the United States in October 2023, which expanded military and security cooperation to include cybersecurity, involving agencies like the U.S. Department of Homeland Security (DHS) in combating shared threats like ransomware. Morocco has also formalized cooperation with India, signing an MoU in September 2025 on cybersecurity and cyber defense, and with the United Arab Emirates (UAE) via an MoU in October 2023 to address growing challenges. Moreover, cooperation with the European Union (EU) is ongoing, primarily through active collaboration with Europol on cybercrime, counter-terrorism, and the exchange of digital evidence, alongside Morocco's efforts to align its data protection standards with the EU's General Data Protection Regulation (GDPR).

Risks:

Future attacks

The enduring risk of the recent attacks lies in how this stolen data can be used for future attacks. The sensitive personally identifiable information (PII) and financial data constitute a long-term social engineering threats, providing a rich source for social engineering, phishing, and identity theft that can be used to compromise banks, corporations, and individuals for years to come. This makes the CNSS breach a precursor to future financial crimes and a clear signal that the private financial sector cannot afford to be complacent.

Legacy systems

Another significant risk to Morocco's cybersecurity is the continued reliance on outdated systems in vital sectors, which leaves them exposed to long-standing technical gaps and vulnerabilities. This is compounded by limited budgets allocated for upgrading digital infrastructure and establishing advanced monitoring centers capable of real-time threat response. The pervasive under-investment in cybersecurity is highlighted by a systemic lack of prioritization among private enterprises and civil society organisations.

Exposure through high stake events

Hosting high-profile events like the AFCON and World Cup places Morocco directly in the global spotlight, making it a primary target for a variety of threat actors, from geopolitical rivals to financially motivated cybercriminals. These global spectacles serve as a high-stakes stress test of Morocco's digital and physical resilience, providing a unique platform to showcase its capabilities on the international stage. The threat landscape is rapidly evolving with the proliferation of advanced technologies, the increasing sophistication of these threats complicates the challenge for Morocco, as a reactive defense posture will be insufficient to counter attacks that are faster and more complex than ever before

FORESIGHT

The CNSS breach was a painful lesson, but it also served as the final piece of evidence proving that a national cybersecurity strategy based voluntary adherence is insufficient. The pervasive apathy among businesses, where over half "do not care about cybersecurity" even after being informed of their vulnerabilities, demonstrates a profound and systemic failure to cultivate a culture of accountability. A national strategy is only as strong as its weakest link, and Morocco’s digital defense cannot rely on hope alone. A plausible future for Morocco's cybersecurity landscape is one where the DGSSI, is granted the legal teeth to enforce compliance across all critical infrastructure, public administrations, and private companies. The idea is to move to institutionalizing a true "carrot and stick" approach. The "stick" would be the power to impose sanctions and fines on entities that fail to conduct mandatory cyber audits, to implement security measures, or to report incidents as required by law. This would compel compliance from those who currently choose to ignore their cybersecurity vulnerabilities, forcing a behavioral change where awareness campaigns have failed. On the other hand, the "carrot" would be the DGSSI’s role in providing the means to achieve compliance. This includes leveraging its existing training center to mandate and certify specialized cybersecurity training for key personnel in critical sectors.

Furthermore, DGSSI certification would become a prerequisite for both public and private entities, ensuring a standardized, high level of security maturity across the board. This future is not a radical departure from Morocco's current path, but a natural and necessary evolution. It is a future where the nation’s strategic readiness is finally matched by its operational resilience.

Global Governance & Sovereignty Foundation

5 rue Ibn Tofaïl. Les Orangers,
10060, Rabat
Maroc

amoutaib@ggs.foundation
+212 537 73 45 13

Konrad-Adenauer-Stiftung e.V.

N. 24 Angle Av. Abdelkrim Benjelloun et Rue Mly. Yaacoub, B.P. 559 Hassan-Rabat
10010, Rabat, Maroc

steven.hoefner@kas.de
+212 537 76 12 32 / 33