ITJ | The International Tax Journal

When learning organizations meet artificial intelligence: Reimagining cybersecurity governance for Algeria

Fathi Daghrir [1], and **Antar Zerrougui** [2]

[1] Mohamed Cherif, Mesaadia University, Souk Ahras, Algeria.
Email: fathi.daghrir@univ-soukahras.dz
[2] University of Continuing Education, Didouche Mourad, Algeria.
Email: antarzerrougui@protonmail.com

Abstract---What happens when we combine the timeless wisdom of organizational learning with the raw power of artificial intelligence to tackle national cybersecurity? This paper explores that question through a conceptual framework we developed specifically for Algeria. We started by examining Algeria's digital landscape and found that while the country is rapidly modernizing, its cybersecurity approach tends to be reactive and fragmented. Our proposed solution is a three-layer architecture that moves beyond simple compliance, aiming instead to create a system that actually learns from its experiences. The framework draws inspiration from international standards but focuses on Algeria's particular challenges with digital sovereignty. What we're offering here is essentially the blueprint theoretical foundation for research that will, in future work, test whether this approach can work in practice.

Keywords---Artificial Intelligence, Cybersecurity Governance, Learning Organization, Decision Support Systems, Digital Sovereignty, Algeria, Adaptive Security, Institutional Learning.

1 Introduction

Artificial intelligence is changing everything, and organizational learning is no exception. In high-stakes fields like cybersecurity, where threats evolve faster than policies can be written, traditional approaches are showing their limits. The old model of waiting for an attack and then

How to Cite:
Daghrir, F., & Zerrougui, A. (2025). When learning organizations meet artificial intelligence: Reimagining cybersecurity governance for Algeria. *The International Tax Journal*, *52*(6), 4258–4265. Retrieved from https://internationaltaxjournal.online/index.php/itj/article/view/406

The International tax journal ISSN: 0097-7314 E-ISSN: 3066-2370
Submitted: 11 February 2025 | Revised: 23 May 2025 | Accepted: 11 November 2025

responding feels increasingly inadequate against threats that adapt in real-time. We're reaching a point where we need to rethink cybersecurity governance entirelynot just adding AI as another tool, but using it to help organizations learn and adapt in ways that were previously impossible.

1.1 *The Algerian Context: A Problem of Modernization*

Algeria finds itself in a tricky position. On one hand, there's tremendous momentum behind digital transformatione-government, smart infrastructure, financial digitization. These initiatives promise real economic and social benefits. On the other hand, each new digital system expands what security experts call the "attack surface," creating more opportunities for cyber threats. From our analysis, three persistent problems seem to undermine Algeria's digital resilience:

1. **Institutional Fragmentation:** Different ministries and agencies often operate in isolation, leading to duplicated efforts and inconsistent responses when threats emerge.
2. **Technological Dependencies:** There's heavy reliance on foreign cybersecurity solutions, which creates strategic vulnerabilities and limits Algeria's ability to cus- tomize defenses to local needs.
3. **The Learning Deficit:** Perhaps most fundamentally, cybersecurity incidents tend to be treated as one-off crises rather than learning opportunities. The same types of attacks succeed repeatedly because there's no systematic process for extracting lessons and improving defenses.

These challenges are particularly acute given Algeria's regional ambitions and strate- gic position. The current reactive stance simply can't keep pace with the speed and sophistication of modern cyber threats.

1.2 *Where Previous Research Falls Short*

While there's no shortage of research on learning organizations or AI in cybersecurity, few studies have brought these domains together in a meaningful way, especially for countries like Algeria that are trying to establish digital sovereignty. Most existing work treats AI as just another piece of technology or discusses learning organizations as a theoretical concept, without showing how they might actually work together in the messy reality of national cybersecurity. Our research attempts to bridge this gap in a few ways:

- We've developed a model that connects AI governance with learning organization theory in the specific context of cybersecurity resilience.
- We've looked closely at Algeria's digital sovereignty situation relative to international standards like the EU NIS2 Directive and OECD AI Principles.
- We've identified what we see as the main institutional and technological barriers to cybersecurity modernization in Algeria.
- Perhaps most importantly, we've laid out a clear path for future research to build on this foundation.

1.3 *Why This Combination Matters*

Bringing AI and organizational learning together represents more than just a technical upgradeit's a different way of thinking about cybersecurity governance. Instead of static policies that gather dust between revisions, we're talking about systems that can learn from each incident, anticipate new threats, and adapt accordingly. This shift feels essential for countries like Algeria that want genuine digital sovereignty rather than just buying the latest security products from abroad.

From a theoretical standpoint, our work extends learning organization theory into the AI era, showing how machine learning might enhance how organizations adapt and create knowledge.

Practically, it offers policymakers and security professionals a concrete framework for building cybersecurity institutions that learn and improve over time.

2 Literature Review

2.1 *The Landscape of Cybersecurity Governance*

Cybersecurity governance has evolved into a complex field involving structures, processes, and policies aimed at protecting digital assets and maintaining system resilience. Several international frameworks have emerged as standards, though each comes with its own assumptions and limitations when applied outside their original context.

The **EU NIS2 Directive** represents Europe's latest attempt to strengthen cyberse- curity across essential services. It casts a wider net than its predecessor, covering more sectors and demanding stricter risk management and incident reporting. While ambi- tious, its implementation in non-EU contexts raises questions about compatibility with local institutional arrangements.

The **NIST Cybersecurity Framework** has gained popularity for its flexibility. Its five functionsIdentify, Protect, Detect, Respond, Recoverprovide a sensible structure, but its voluntary nature means it relies heavily on organizational buy-in that may be uneven in fragmented governance environments.

ISO/IEC 27035 offers detailed guidance on incident management, emphasizing learn- ing from security events. However, its comprehensive approach assumes a level of organi- zational maturity that may not yet exist in developing cybersecurity ecosystems.

What these frameworks share is a recognition that cybersecurity requires systematic management. Where they often fall short is in accounting for the specific institutional and technological constraints of countries building their digital infrastructure from the ground up.

2.2 *AI in Cybersecurity: Promise and Peril*

The integration of AI into cybersecurity operations brings both exciting possibilities and serious concerns that we're only beginning to understand.

On the positive side, AI can identify subtle patterns in vast datasets that human analysts might miss, potentially detecting sophisticated attacks that would slip past tra- ditional signature-based systems. Machine learning algorithms can automate routine se- curity tasks, freeing up human experts for more complex analysis. They can also help with proactive threat hunting and adaptive authentication. But the challenges are significant:

- **Adversarial Exploitation:** Attackers can deliberately manipulate AI systems through techniques like data poisoning or model evasion.
- **Data Hunger:** AI models require massive amounts of high-quality training data, which may be scarce in certain cybersecurity contexts.
- **The Black Box Problem:** Some AI systems arrive at conclusions through pro- cesses so complex that even their creators struggle to explain them, raising obvious accountability issues.
- **Context Blindness:** Current AI often misses the nuanced understanding that human experts bring to complex situations, particularly with novel threats.

These limitations suggest that AI's role in cybersecurity should be one of augmentation rather than replacementa tool that enhances human judgment rather than supplants it.

2.3 *Learning Organizations Meet Cybersecurity*

The concept of learning organizations, pioneered by Senge's work on systems thinking and mental models [1], emphasizes continuous adaptation and knowledge creation. Nonaka and Takeuchi extended this with their theory of knowledge conversion between tacit and explicit forms [2].

In cybersecurity, this perspective encourages a shift from simply putting out fires to building institutions that learn from each incident. It involves what Argyris called "double-loop

learning"questioning underlying assumptions rather than just fixing surface problems. When a bank suffers a phishing attack, for instance, a learning organization wouldn't just reset the compromised accounts; it would examine why its training, technical controls, or culture allowed the attack to succeed in the first place.
AI technologies could potentially accelerate this learning by helping organizations spot patterns across incidents, extract knowledge from security data, and even suggest improvements to policies and procedures. The result might be what we're calling "AI- augmented learning organizations" in cybersecurityinstitutions that learn faster and more systematically than would otherwise be possible.

2.4 *The Complicated Reality of Digital Sovereignty*

Digital sovereigntya nation's ability to control its digital infrastructure, data flows, and technological developmenthas become a pressing concern as countries recognize their vul- nerability to external pressures and dependencies [4].
For countries like Algeria, this isn't just an abstract concept. It means:

- **Infrastructural Control:** Owning or having reliable access to telecommunications networks, data centers, and other critical digital infrastructure.
- **Data Governance:** Making decisions about where data is stored, how it's pro- cessed, and who can access it.
- **Technological Self-Reliance:** Developing enough local expertise and capacity to reduce dangerous dependencies on foreign technologies.

The **African Union Convention on Cybersecurity** (Malabo Convention) repre- sents a regional effort to address these concerns through harmonized frameworks and capacity building [9]. Similarly, the **OECD AI Principles** advocate for AI systems that respect human rights and democratic values [10]. Both initiatives recognize that technological adoption without strategic autonomy creates its own vulnerabilities.

2.5 *The Double-Edged Sword of AI*

AI's dual-use naturethe same technology that can defend networks can also be weaponized to attack themcreates ethical dilemmas that go beyond technical considerations. Respon- sible AI governance in cybersecurity means confronting several uncomfortable questions:

- How do we ensure AI systems operate within ethical boundaries, especially when they're used for national security?
- Who is accountable when an AI system makes a mistake that leads to a major security breach?
- Can we make AI decisions transparent enough to maintain public trust?
- How do we build AI systems resilient enough to withstand determined adversaries?

These questions don't have easy answers, but they can't be ignoredespecially in na- tional cybersecurity contexts where mistakes can have serious consequences for both se- curity and civil liberties.

3 Algeria's Cybersecurity Landscape

If you examine Algeria's cybersecurity ecosystem through official documents and public statements, you see a system that appears reasonably well-structured. There's a cy- bersecurity law (18-05 from 2018), a High Council for Cybersecurity providing strategic direction, and a national CERT (ALCERT) handling incident response. The basic com- ponents, at least on paper, seem to be in place.

But looking closer reveals a more complicated picture. Our analysis, based on policy documents and conversations with professionals in the field, suggests that these insti- tutions often operate with limited coordination. The High Council sets policy, but its connection to the day-to-day work of various ministries and sector regulators can be ten- uous. ALCERT does valuable work on incident response, yet its effectiveness is sometimes hampered by unclear mandates and resource constraints.

3.1 *The Legal Framework: Strong Foundations, Weak Imple- mentation?*

Algeria's primary cybersecurity legislation, Law 18-05, established the legal basis for pro- tecting national information systems and critical infrastructure. It was an important step forward when passed in 2018, defining cybercrimes and outlining institutional responsi- bilities [5].
However, the law's practical implementation has faced several challenges:

- **Emerging Technology Gaps:** The legislation doesn't fully address newer tech- nologies like cloud computing, IoT devices, or AI systems, creating regulatory am- biguities.
- **Enforcement Inconsistencies:** Enforcement capacity varies significantly across sectors and regions, undermining the law's effectiveness.
- **International Compatibility:** Partial alignment with international standards creates complications for organizations operating across borders.

More recent decrees like 23-406 have attempted to provide implementation details, but their impact remains unclear as the practical rollout continues.

3.2 *Institutional Architecture: Many Players, Uncertain Coor- dination*

Algeria's cybersecurity institutions reflect a centralized model in theory but often function in a fragmented way in practice:

- **High Council for Cybersecurity (HCC):** Sits at the top of the policy pyramid but lacks direct operational authority, which can make its strategic guidance feel disconnected from ground-level realities.
- **Algerian Computer Emergency Response Team (ALCERT):** Plays a crucial role in incident response but sometimes struggles with jurisdictional ambiguities and competing priorities across different sectors.
- **Sectoral Regulators:** Various ministries and regulatory bodies maintain their own cybersecurity responsibilities, leading to potential coordination problems and uneven capabilities.
- **Law Enforcement:** Specialized cybercrime units exist but face technical capacity challenges and growing case backlogs.

This institutional landscape shows growing awareness of cybersecurity threats but suffers from the classic problem of siloed operations and unclear lines of authority.

3.3 *Infrastructural Dependencies: A Sovereignty Challenge*

Algeria's digital infrastructure reveals significant dependencies that complicate both se- curity and sovereignty:

- **Telecommunications:** Heavy reliance on imported networking equipment with limited local manufacturing or customization capabilities.
- **Security Solutions:** Predominance of international vendors in critical infrastruc- ture protection, creating potential supply chain risks.
- **Cloud Services:** Growing use of international cloud providers raises questions about data jurisdiction and control.
- **Technical Expertise:** A noticeable skills gap in advanced cybersecurity domains like threat intelligence and digital forensics.

While there are initiatives to develop national data centers and local capabilities, the path to genuine technological sovereignty appears long and resource-intensive.

3.4 *Operational Realities: Reacting Rather Than Anticipating*

Algeria's cybersecurity operations have improved over time but remain predominantly reactive:

- **Threat Intelligence:** Limited systematic collection and analysis of threat data hinders the ability to anticipate attacks rather than just respond to them.
- **Incident Response:** The focus remains on containing individual incidents rather than extracting broader lessons that could prevent future occurrences.
- **Risk Management:** Approaches tend to be compliance-focused rather than continuously adaptive based on changing threat intelligence.
- **Coordination:** Cooperation between entities often happens on an ad-hoc basis during major incidents rather than through established, regularly exercised proto- cols.

These operational patterns reflect deeper systemic challenges in developing mature cybersecurity capabilities.

3.5 *The Core Challenges*

Our analysis points to several interconnected problems that undermine Algeria's cyber- security resilience:

- **Institutional Fragmentation:** Different parts of the system often work at cross- purposes or duplicate efforts.
- **Coordination Deficits:** No single entity has both the strategic vision and opera- tional authority to drive a unified national approach.
- **Information Silos:** Restrictive data policies and technical barriers prevent the sharing of threat intelligence that's essential for collective defense.
- **Workforce Gaps:** Insufficient specialized education and professional development opportunities constrain capability building.
- **Innovation Constraints:** Limited investment in cybersecurity R&D, particularly around emerging technologies like AI, hinders local innovation.

Together, these challenges create an environment where cybersecurity efforts remain largely reactiveprecisely the problem our proposed framework attempts to address.

4 Toward an AI-Enabled Learning Architecture

Faced with these challenges, we asked a simple but fundamental question: what would it take to build a cybersecurity system that doesn't just respond to threats but actually learns and adapts over time? The model we're proposing consists of three interconnected layers, each building on the last to create what we hope could become a continuous learning cycle.

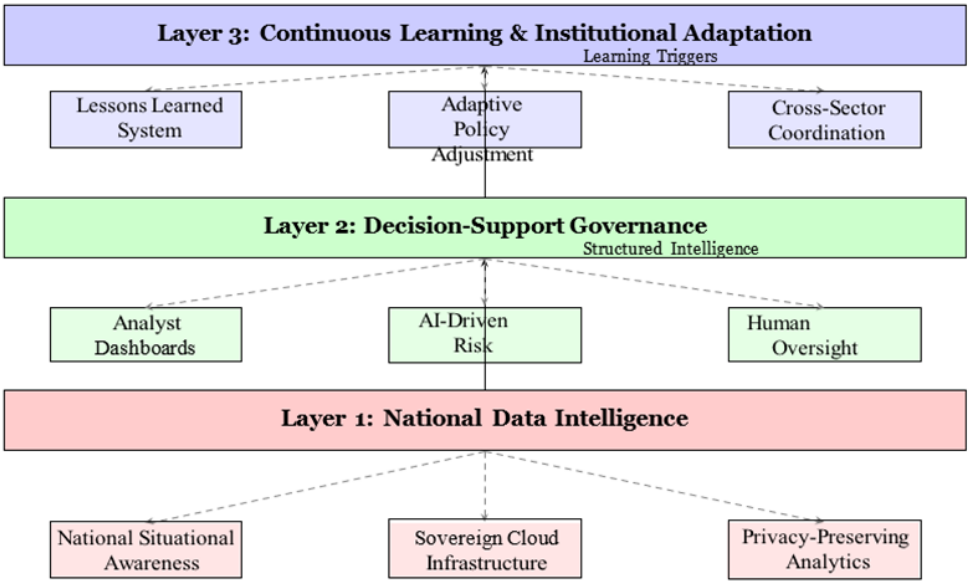

Figure 1: A Three-Layer Architecture for Cybersecurity That Learns

4.1 *Layer 1: Making Sense of the Data*

Think of this as the foundationthe layer that tries to make sense of all the cybersecu- rity data currently scattered across different agencies and sectors. Right now, threat information exists in silos: network logs here, security alerts there, vulnerability reports somewhere else. Our first layer proposes creating a centralized platform that can aggre- gate and correlate this information to build a real-time picture of what's happening across the national digital landscape.

Of course, collecting this much data immediately raises legitimate concerns about privacy and sovereignty. We're not suggesting a massive surveillance apparatus. Instead, the model emphasizes using what's often called "sovereign cloud infrastructure"nationally controlled data centersto ensure sensitive information stays within Algerian jurisdiction. Techniques like differential privacy could help the system identify national-level attack patterns without exposing sensitive details about specific organizations or individuals. It's a difficult balance to strike, but one we believe is necessary for effective defense.

4.2 *Layer 2: Supporting Human Decisions*

Raw data, even in massive quantities, isn't particularly useful on its own. This middle layer is about turning that data into actionable insights for the people who need to make decisionssecurity analysts, IT managers, policy makers. Here, AI could serve as a powerful assistant, though certainly not a replacement for human judgment.

We imagine interactive dashboards that visualize the threat landscape in intuitive ways, showing emerging patterns and potential impacts. AI models could provide dy- namic risk assessments for critical infrastructure, helping organizations prioritize their limited security resources where they're needed most. Perhaps most usefully, this layer could include AI-assisted incident triage. Instead of a human analyst being buried under thousands of low-priority alerts, the system could automatically filter and escalate only the most serious incidents based on predefined criteria.

A key principle here is that the AI *suggests* rather than *commands*. Human oversight is built directly into the design. For any significant decisionlike taking a critical system offlinea human must remain in the loop. The goal is to augment human intelligence, not replace it.

4.3 *Layer 3: Building Institutional Memory*

This is where the "learning organization" concept truly comes to life. It's also, we admit, the most ambitious part of our proposal.

The objective here is to ensure that the system actually learns from its experiences and adapts accordingly. After a significant cybersecurity incident is contained, the process shouldn't simply end. A structured "lessons learned" analysis would be automatically triggered, feeding directly into updates for detection systems, policy adjustments, and even training programs for security staff.

The real test of this layer is whether it can overcome what we might call institutional inertia. Can an AI's analysis showing that a particular security policy is ineffective ac- tually lead to that policy being revised? We propose creating formal feedback loopswhat we're calling "cross-sector coordination loops"where insights from, say, a telecommunica- tions breach are automatically shared with the financial sector, allowing all parts of the
system to raise their defenses together. It's about creating what amounts to an institu- tional memory for cybersecurity, one that grows smarter with each experience.

4.4 *Making the Pieces Work Together*

Individually, these layers each offer some value. But their real potential emerges from how they connect to each other. The learning from Layer 3 should refine the AI models in Layer 1. The intelligence from Layer 1 should inform the decisions in Layer 2. It's meant to be a continuous cycle of gathering intelligence, making decisions, and adapting based on what's learned.

While this remains a conceptual framework for now, we believe it points toward a more dynamic approach for Algeriaand perhaps other countries facing similar challengesto build cybersecurity capabilities that aren't just strong, but intelligently and resiliently so.

Acknowledgments

We're grateful to the many cybersecurity professionals within Algerian institutions who shared their time and insights, helping us understand both the challenges and opportu- nities in the current system. This research wasn't supported by any specific grant, which perhaps gave us more freedom to explore unconventional ideas.

References

[1] Senge, P. M. (1990). *The Fifth Discipline: The Art and Practice of the Learning Organization*. Doubleday.

[2] Nonaka, I., & Takeuchi, H. (1995). *The Knowledge-Creating Company: How Japanese Companies Create the Dynamics of Innovation*. Oxford University Press.

[3] Jordan, M. I., & Mitchell, T. M. (2015). Machine learning: Trends, perspectives, and prospects. *Science*, 349(6245), 255-260.

[4] DeNardis, L. (2020). *The Internet in Everything: Freedom and Security in a World with No Off Switch*. Yale University Press.

[5] Algerian Government. (2018). *Law 18-05 on Cybersecurity*. Official Journal of the Algerian Republic.

[6] European Union. (2022). *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive)*.

[7] National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity*. Version 1.1.

[8] International Organization for Standardization. (2016). *ISO/IEC 27035-1:2016 Infor- mation technology Security techniques Information security incident management*.

[9] African Union. (2014). *African Union Convention on Cyber Security and Personal Data Protection*.

[10] OECD. (2019). *Recommendation of the Council on Artificial Intelligence*.