7 ISLANDS
DEFENSE & INTEL

Why we deliberately avoid the term “MENA” in cybersecurity analysis

Author: *Nicolas Duguay, Founder, 7 Islands Defense & Intel*

Date: *January 2026*

The term “MENA” is convenient. It is widely used across policy papers, investment decks, media narratives, and market reports. It creates the impression of coherence where none exists. For cybersecurity analysis, that convenience is not neutral. It is actively misleading.

We deliberately avoid the term “MENA” because it collapses fundamentally different institutional cyber regimes into a single analytical category. In doing so, it erases the very factors that determine whether cybersecurity capabilities are produced, adopted, sustained, or fail in practice.

Cybersecurity is not shaped primarily by geography or culture. It is shaped by institutions: how power is distributed, how responsibility is assigned, how risk is owned, how technology is governed, and how decisions survive over time. When viewed through this lens, grouping Israel, Gulf states, Levantine regimes, and North African administrations under a single label obscures more than it reveals.

Israel is a cyber production ecosystem. It is defined by deep integration between national security institutions, intelligence services, talent circulation, and export-oriented technology development. Cyber capability there is generated upstream, then projected outward. Treating Israel as part of a regional “market” alongside countries whose cyber posture is primarily acquisitive or externally dependent misunderstands its role entirely.

Much of the Middle East operates under a different logic altogether. Cyber adoption is often centralized, decision-driven, and politically accelerated. Capabilities can be deployed quickly, sometimes at impressive scale, but institutionalization frequently lags behind acquisition. Authority is concentrated. Accountability is narrow. Sustainability depends heavily on external vendors and continued political sponsorship. This produces speed, but also fragility.

North Africa follows yet another pattern. Cybersecurity there is constrained by legacy administrative structures, limited budgets, dependency on foreign technologies, and overlapping security mandates. Adoption is cautious, incremental, and often shaped more by institutional survivability than by strategic ambition. Expectations are high, capacity is uneven, and risk tolerance is low. The governing logic is neither export-driven nor acceleration-focused, but defensive and absorptive.

Lumping these environments together under “MENA” suggests a shared market logic that does not exist. It encourages vendors to generalize go-to-market strategies, investors to misread adoption signals, and policymakers to project assumptions across incompatible systems. The result is repeated confusion: pilots that do not scale, partnerships that stall, and technologies that perform well on paper but fail institutionally.

The persistence of the MENA label reflects external needs more than regional realities. It simplifies mapping for outsiders. It aligns with geopolitical shorthand. It reduces complexity for reporting and benchmarking. But cybersecurity does not reward simplification. It rewards institutional precision.

For this reason, we treat Israel, the Middle East, and North Africa as distinct analytical environments, not subregions of a single market. Each operates under different constraints, incentives, and failure modes. Each requires its own interpretive framework.

Using “MENA” as a cyber category is not just imprecise. It is analytically unsafe.

Editorial note —
This analysis reflects observations informed by institutional and operational exposure across defense-adjacent security and cybersecurity environments.

For discussion only; not operational guidance.

The original version of this text was written in French and translated into English with the assistance of AI-based tools.