7 ISLANDS
DEFENSE & INTEL

Israel: a cyber origin ecosystem, not a market

***Abstract**: Israel is routinely treated as a cybersecurity market, when it functions primarily as a production environment for capabilities, companies, and operational doctrine. This misreading explains why market-entry logic consistently underperforms there.*

***Why this matters**: Because Israel does not behave like a demand-driven cyber market, and strategies built on that assumption almost always misfire.*

***Who this is for**: Actors engaging Israeli cyber environments while expecting buyer behavior, procurement pathways, or scalable local adoption.*

***What to watch for**: Sustained engagement without conversion is not a signal problem; it is usually a category error.*

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

***Date** : January 2026*

Israel is often described as a cybersecurity market, but the term fits poorly. Markets are shaped by demand, absorption capacity, and purchasing logic. None of these elements meaningfully structure the Israeli cyber environment. What exists instead is a dense production system that continuously generates capabilities, companies, and operational approaches, largely independent of local consumption needs.

Cybersecurity in Israel is not organized around procurement cycles or buyer segmentation. It is anchored in a tight institutional continuum that links intelligence units, military organizations, national security bodies, academia, and venture capital. Individuals move through these structures quickly, carrying operational assumptions with them. What is learned under constraint is not abstracted into doctrine and later commercialized; it is commercialized directly. The boundary between operational exposure and product development is thin, often nonexistent.

As a result, Israel produces far more cyber capability than it can plausibly consume internally. This is not an imbalance to be corrected. It is the system's defining feature.

Domestic adoption is therefore a weak signal. Capabilities do not need to be "proven" locally in the way foreign vendors often expect. Operational relevance is established upstream, long before anything reaches a sales process. By the time a product exists, it has usually already been shaped by environments that resemble high-friction deployment conditions more closely than most institutional buyers elsewhere.

This is where external actors begin to misread what they are seeing.

Engagement with Israeli cyber actors is often intense and substantive. Discussions move quickly to architecture, constraints, edge cases, failure modes. Feedback is direct and technically grounded. From the outside, this looks like traction. It is not. It is diagnostic behavior. Interest reflects curiosity and comparative evaluation, not buying intent. Conversion is not the default outcome of engagement because purchase is not the primary validation mechanism.

Procurement does exist, but it plays a secondary role. External solutions are not evaluated as answers to unmet needs, but as marginal contributors to an environment that is already saturated with internally generated capability. Novelty carries little weight. Even technical excellence is insufficient if it does not align cleanly with existing operational logic, governance expectations, and long-term autonomy requirements.

Export orientation further distorts outside perception. Most Israeli cyber companies are not built for Israel. They are designed for deployment elsewhere, often in environments with slower decision-making, weaker institutional coupling, or lower baseline maturity. Israel functions as an origin point, not as a destination. Success is measured by external adoption, not domestic penetration.

This creates a recurring paradox. Israel is open, accessible, and unusually transparent at the technical level. At the same time, it is structurally closed as a market. Openness signals analytical interest, not commercial demand. Vendors accustomed to demand-driven environments routinely interpret sustained dialogue as progress, only to discover that no procurement pathway ever materializes.

Governance expectations reinforce this dynamic. Cybersecurity is embedded in national security thinking rather than treated as a compliance or IT function. Accountability is direct. Failure is tangible. Institutional tolerance for technical complexity is high, but tolerance for external dependency is low. Solutions that introduce governance ambiguity, opaque control, or long-term vendor reliance generate friction regardless of their technical merit.

This is also why "best-of-breed" narratives land poorly. Israeli environments are already accustomed to assembling, modifying, and discarding components as conditions change. Coherence is maintained through people, shared assumptions, and institutional memory rather than through vendor-managed stacks. Solutions that presume static architectures or standardized workflows struggle to integrate meaningfully, not because they are flawed, but because they are misaligned with how control is actually exercised.

The pattern is consistent across engagements.

Actors who approach Israel as a market to penetrate often leave frustrated by the absence of conversion. Those who recognize it as an origin ecosystem engage differently. They seek signal,

positioning, partnership, or downstream leverage. They do not expect volume, and they do not mistake interaction for demand.

Israel does not need to buy in order to validate itself. It already operates inside its own reference frame.

Understanding this does not make engagement easier. It makes outcomes legible.

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.