7 ISLANDS
DEFENSE & INTEL

Why comparing cyber markets by size is the fastest way to misread them

Abstract: *Market size comparisons obscure more than they reveal in cybersecurity. What determines outcomes is not total spend, but how decisions are made, how risk is owned, and how institutions absorb capability over time.*

Why this matters: *Because size-based comparisons lead companies to pursue the wrong markets with the wrong assumptions, often at the wrong time.*

Who this is for: *Executives, investors, and market-entry teams evaluating where—and how—to deploy cybersecurity capabilities internationally.*

What to watch for: *If your prioritization logic starts with TAM figures rather than decision structure and adoption pathways, you are likely optimizing for visibility, not outcomes.*

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

Date: *January 2026*

Cybersecurity markets are routinely compared by size. Total addressable market. Annual spend. Growth rate. Share of global investment. These figures dominate board discussions, investor decks, and expansion strategies. They are easy to communicate and reassuringly quantitative.

They are also a poor proxy for how markets actually behave.

In cybersecurity, market size tells you almost nothing about how adoption occurs, how long it takes, or how durable outcomes will be once achieved. Two markets of identical monetary size can behave in radically different ways depending on governance structure, institutional maturity, procurement logic, and risk ownership. Treating size as a primary comparative variable therefore produces a systematic distortion of expectations.

The first problem is that “market size” collapses fundamentally different forms of demand into a single number. Public-sector procurement, regulated critical infrastructure, private enterprise

spending, and services consumption are often aggregated despite operating under incompatible logics. A dollar spent on managed detection services in a regulated utility does not behave like a dollar spent on endpoint software in a venture-backed enterprise. Aggregating them creates the illusion of coherence where none exists.

This illusion becomes especially misleading in institutional environments.

Large cybersecurity markets often appear attractive precisely because they contain many buyers. In practice, those buyers may be constrained by overlapping jurisdictions, centralized shared services, or procurement frameworks designed to limit variance rather than enable rapid choice. What looks like scale on paper may translate into a narrow set of viable entry points, long decision cycles, and high sensitivity to misalignment. Market size does not mitigate these constraints. It often amplifies them.

Conversely, smaller markets are frequently dismissed as secondary. Yet markets with limited size but clear governance, concentrated decision authority, and coherent procurement pathways can absorb new capabilities more efficiently. Adoption may be slower initially, but once achieved it tends to be more stable. Size, in this sense, is less predictive than structure.

Another distortion arises from conflating spending potential with spendability.

Cybersecurity budgets are not free-floating pools of capital. They are embedded in institutions with competing priorities, political exposure, and accountability obligations. A market may be “large” in aggregate while remaining highly resistant to new entrants whose offerings disrupt established narratives, tooling baselines, or assurance frameworks. The existence of money does not imply accessibility. In some environments, increased spending correlates with increased conservatism, not openness.

Size comparisons also obscure the role of services.

In many mature cyber markets, a significant portion of spend flows toward integration, operations, and managed capability rather than product acquisition. Vendors interpreting headline figures as product opportunity routinely misallocate effort. They optimize for feature differentiation while institutions are optimizing for operational continuity. The result is a persistent mismatch between what is sold and what is absorbed, regardless of market scale.

There is also a temporal problem.

Market size snapshots flatten time. They ignore how long it takes to move from interest to adoption, from pilot to baseline, from reference to renewal. A smaller market with predictable cycles and low reversal risk may outperform a larger market characterized by churn, stalled initiatives, and frequent resets. Speed of entry and durability of position matter at least as much as aggregate volume.

This is particularly relevant in cross-border comparisons.

The temptation to rank markets—United States first, then Europe, then “secondary” jurisdictions—rests on an assumption that scale determines leverage. In practice, leverage emerges from institutional fit. Companies that succeed internationally tend to treat markets not as targets ranked by size, but as systems ranked by compatibility with their delivery model, governance posture, and tolerance for ambiguity.

What size-based comparisons consistently miss is the cost of misalignment.

Entering a large market with the wrong assumptions is not neutral. It consumes time, credibility, and organizational focus. Failed or stalled engagements leave traces. Procurement memories persist. Re-entry is rarely clean. Smaller, more selective markets often function as proving grounds not because they are easier, but because they enforce discipline early. Capabilities that survive these environments tend to travel better later.

None of this is an argument against ambition.

It is an argument against reductionism.

Cybersecurity markets are institutional systems before they are economic ones. Their behavior is shaped by how risk is perceived, who carries responsibility, and how failure is absorbed. These variables do not scale linearly with spend. They vary discontinuously across jurisdictions, sectors, and governance cultures.

Comparing cyber markets by size alone is therefore not just simplistic. It is actively misleading.

It encourages companies to optimize for where the money appears to be, rather than for where adoption is structurally possible. It privileges visibility over viability. And it explains why so many well-capitalized market-entry efforts generate activity without conversion.

Markets are not defined by how much they spend.

They are defined by how they decide.

Ignoring that distinction is the fastest way to misunderstand them.

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.