7 ISLANDS
DEFENSE & INTEL

Why the U.S. cybersecurity market looks fast – and traps the unprepared

Abstract: *The U.S. cybersecurity market rewards speed, scale, and narrative momentum, but punishes actors who mistake early access for durable institutional adoption.*

Why this matters: *Because early traction in the U.S. often conceals structural fragility that only appears once scale, liability, and accountability converge.*

Who this is for: *Foreign vendors, investors, and advisors engaging U.S. federal, defense-adjacent, and regulated cyber environments.*

What to watch for: *If momentum substitutes for institutional anchoring, growth will stall precisely when stakes become real.*

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

Date: *January 2026*

The U.S. cybersecurity market is frequently described as the most dynamic, open, and opportunity-rich environment in the world. In many respects, this description is accurate. Budgets are large. Buyers are numerous. The ecosystem is dense, competitive, and visibly active. Access is comparatively easy. Conversations start quickly. Pilots launch early. Contracts appear achievable. For many foreign companies, the U.S. feels like a market where speed is rewarded and friction is low.

This impression is not false. But it is incomplete.

What the U.S. market offers early is not adoption. It offers velocity. And velocity, in the American cyber ecosystem, is not the same as institutional commitment.

The U.S. system is built to encourage experimentation at scale. Agencies, departments, primes, and commercial actors all operate within frameworks that tolerate parallel initiatives, overlapping pilots, and partial deployments. Failure is accepted, provided it is compartmentalized. This creates

an environment where new technologies can be tested rapidly without immediately triggering full accountability. For vendors, this feels like openness. For institutions, it is a risk management strategy.

The trap lies in misreading this phase.

Early engagement in the U.S. often produces strong signals: enthusiastic technical teams, visible executive sponsorship, inclusion in innovation programs, and positive feedback loops. These signals are real. But they are provisional. They occur upstream of the moment when responsibility hardens—when a solution becomes operationally central, legally exposed, and politically defensible.

That moment is where the U.S. market changes character.

As initiatives scale, decision authority consolidates. Legal, compliance, procurement, and liability functions assert themselves. Risk tolerance drops sharply. What was acceptable as an experiment becomes unacceptable as a dependency. Solutions that thrived in pilot conditions are suddenly evaluated through different lenses: contractual exposure, indemnification, data handling, chain-of-custody, continuity of operations, and failure attribution. The transition is rarely smooth, and many initiatives stall precisely at this inflection point.

This is why the U.S. market produces a distinctive failure pattern. Technologies are not rejected outright. They are overtaken. New initiatives launch before older ones mature. Attention shifts. Budgets are reallocated. Vendors mistake this churn for competition when it is often a byproduct of institutional filtering. What survives is not what moved fastest, but what could withstand scrutiny once experimentation ended.

The structure of the U.S. ecosystem reinforces this dynamic.

Federal agencies operate with significant autonomy, yet under a common legal and political framework. The defense industrial base introduces another layer of mediation, where primes absorb risk on behalf of the state. Commercial critical infrastructure adds yet another logic, shaped by liability exposure, insurance pressure, and shareholder accountability. Across these environments, speed is tolerated early because responsibility is diffuse. Once responsibility concentrates, tolerance evaporates.

Foreign actors often underestimate how abruptly this shift occurs.

U.S. credibility is not cumulative in the way many expect. A successful pilot in one agency does not guarantee legitimacy in another. Commercial traction does not automatically translate into federal trust. References travel, but they do not transfer responsibility. Each institutional context re-evaluates risk independently, often resetting the clock just as vendors believe they are accelerating.

There is also a cultural asymmetry that complicates interpretation. American institutions are comfortable expressing enthusiasm without commitment. Positive language does not imply obligation. Momentum is encouraged precisely because it can be reversed. For outsiders accustomed to more conservative signaling, this creates systematic overconfidence. The market appears receptive long after it has quietly begun to disengage.

Operationally, this produces brittle growth trajectories. Companies scale sales and delivery based on early signals, only to encounter resistance once institutional gravity asserts itself. Costs rise

faster than conversion. Internal narratives emphasize execution problems, while the real issue is misalignment with how the U.S. system transitions from experimentation to ownership.

The companies that endure in the U.S. market tend to follow a different pattern.

They treat early velocity as provisional. They assume that real scrutiny has not yet begun. They invest in legal robustness, compliance depth, and delivery discipline before they appear strictly necessary. They anchor themselves through partners who already carry institutional liability. They prioritize survivability at scale over visibility at speed.

Most importantly, they do not confuse access with adoption.

The U.S. cybersecurity market is not deceptive. It is consistent. It rewards those who understand that openness is a phase, not a state. Speed is tolerated until responsibility becomes unavoidable. At that point, only technologies—and organizations—that can absorb liability, scrutiny, and long-term accountability remain.

The danger is not moving too slowly.

It is moving quickly in the wrong direction.

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.