7 ISLANDS
DEFENSE & INTEL

# The political economy of cyber: who pays, who captures value, and why inefficiency survives

**Abstract**: Cybersecurity is usually discussed in terms of threats, tools, and capabilities. Much less attention is paid to how money, responsibility, and institutional protection actually circulate within the sector. Those flows explain why certain cybersecurity models persist, even when their operational value is limited.

**Why this matters**: Because cybersecurity decisions are shaped less by effectiveness than by who carries cost, who carries risk, and who carries blame.

**Who this is for**: Senior decision-makers, budget holders, procurement leaders, and advisors operating in public-sector, regulated, or defense-adjacent environments who need to understand why cybersecurity behaves the way it does once money, accountability, and scrutiny enter the equation.

**What to watch for**: If cybersecurity spend is justified primarily through risk language and audit alignment, expect operational inefficiencies to persist—by design—regardless of tooling quality or technical maturity.

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

***Date**: January 2026*

---

Cybersecurity is often framed as a strategic necessity. In practice, it behaves more like a negotiated expense, embedded in institutional structures that prioritize continuity and protection over efficiency.

That distinction matters.

Most cybersecurity spending is not driven by a clear link between investment and outcome. It is driven by the need to demonstrate foresight, diligence, and alignment with accepted risk frameworks—especially after something goes wrong.

**Who actually pays**

In most organizations, the people who pay for cybersecurity are not the ones who deal with its daily consequences.

Business units absorb friction. Operators absorb complexity, alert fatigue, and degraded workflows. Yet budgets sit elsewhere—usually with IT, risk, compliance, or executive functions whose primary concern is exposure, not productivity.

This separation is structural. Cybersecurity is funded where accountability is visible, not where the work happens. It survives because it protects the institution from scrutiny, not because it consistently improves operational performance.

**Where value ends up**

Value in cybersecurity does not flow toward those closest to outcomes.

Vendors capture value by aligning their products with recognizable categories: compliance, resilience, zero trust, maturity. Integrators capture value by absorbing complexity and making fragmented systems tolerable to manage. Consultants capture value by producing documents that translate uncertainty into evidence of due diligence.

Operators, despite being essential, capture very little. Their role is treated as an operating cost, not a strategic asset.

This distribution is stable because it matches institutional preferences. Auditable structures, contractual responsibility, and defensible processes matter more than marginal gains in effectiveness.

**Why inefficiency survives**

From the outside, many cybersecurity environments look inefficient. Too many tools. Overlapping controls. Heavy governance. From the inside, much of this is intentional.

Redundancy signals seriousness. Process signals control. Documentation signals responsibility. Systems that are too lean, too elegant, or too dependent on individual expertise are harder to defend when something breaks.

In cybersecurity, inefficiency often functions as insurance. It reduces exposure to blame, even if it increases operational drag. That trade-off is rarely acknowledged, but it shapes most large environments.

**What happens under budget pressure**

Cybersecurity budgets are rarely cut cleanly. They are reshaped.

Spending tied to compliance, reporting, and baseline controls tends to remain. Spending tied to experimentation, customization, or operator comfort is easier to defer. Training is trimmed. Integration depth is reduced. Advanced capabilities are postponed.

Licenses, however, remain. Frameworks remain. External validation remains.

What survives is what supports institutional defensibility.

## Risk as a working language

Over time, cybersecurity has learned how to justify itself. It speaks the language of risk—not as operators experience it, but as institutions can manage it.

That language is abstract enough to travel across silos, formal enough to satisfy oversight, and flexible enough to remain defensible after failure. It has allowed cybersecurity to anchor itself structurally inside organizations.

It has also shifted incentives. Alignment with risk frameworks often matters more than reduced harm. The ability to explain a decision matters more than its practical effect.

Cybersecurity is increasingly about surviving incidents, not preventing them.

## What this produces in the market

Markets shaped by these dynamics reward solutions that fit institutional narratives. They punish solutions that require structural change, even when those solutions work.

This is why some vendors dominate without standing out technically. Why integrators remain central. Why disruptive approaches struggle to scale unless they are reframed as governance improvements.

Cybersecurity markets do not reward efficiency. They reward survivability.

## Closing

Looking at cybersecurity through a political-economic lens does not diminish its importance. It explains its behavior.

Cybersecurity persists because institutions need ways to demonstrate control in environments they cannot fully master. Under scrutiny, what matters is not theoretical effectiveness, but institutional defensibility.

Money flows accordingly.

---

**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.