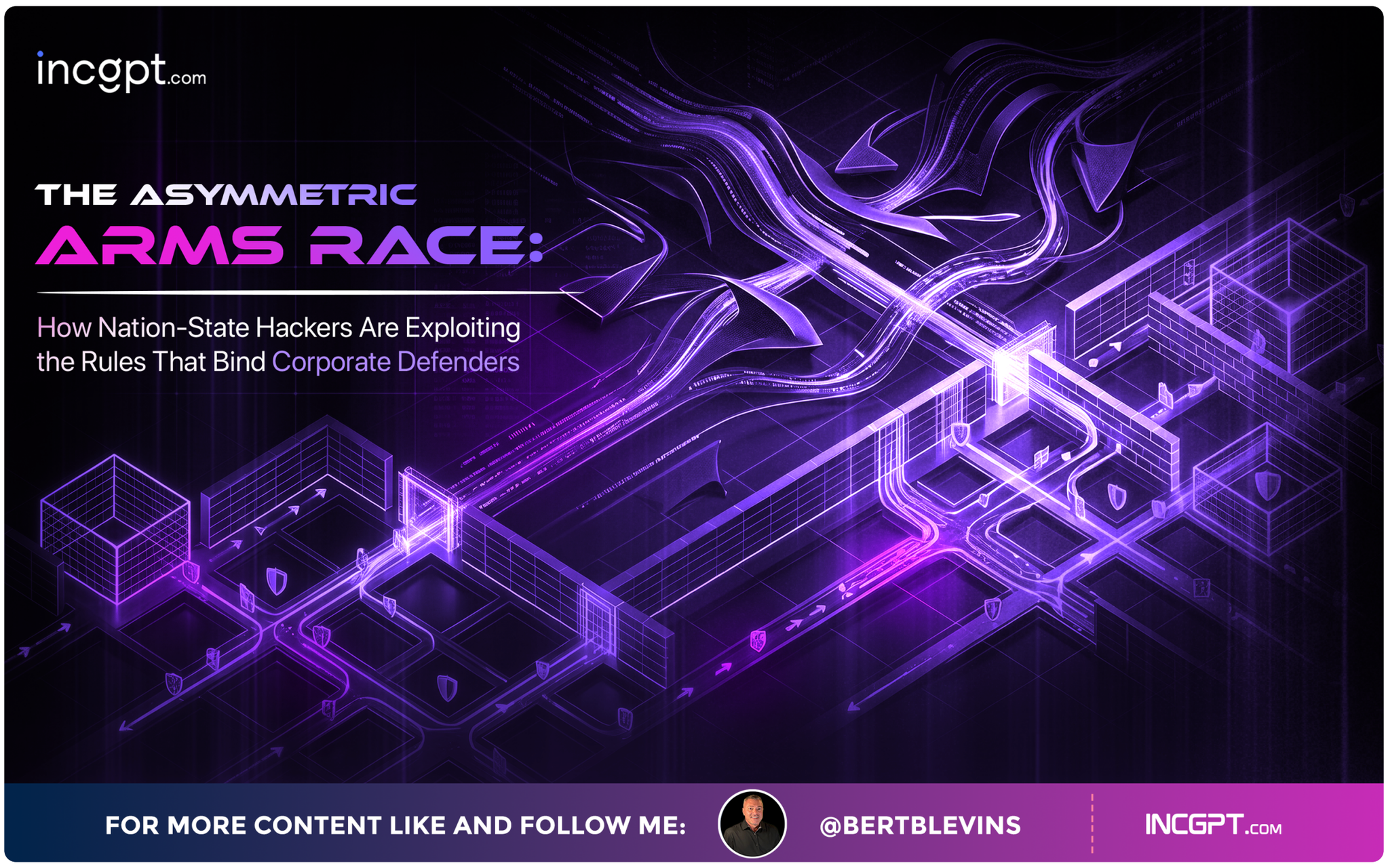
The Asymmetric Arms Race: How Nation-State Hackers Are Exploiting the Rules That Bind Corporate Defenders



When Geopolitics Goes Digital

For decades, geopolitical disputes played out through diplomacy, economic sanctions, and military action. Today, a new front has emerged that is arguably just as destructive and far harder to contain. Cyberattacks launched by nation-state actors have become the weapon of choice for governments looking to retaliate against adversaries while maintaining plausible deniability. The latest wave of incidents tied to the escalating tensions between Iran, Israel, and the United States has made this reality impossible to ignore.

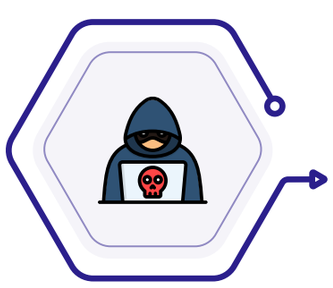
In March 2026, the Iran-linked hacking group Handala claimed responsibility for a massive wiper attack against Stryker, a Michigan-based medical device manufacturer with operations in more than 60 countries. The attackers reportedly gained access to administrative portals and remotely erased data from over 200,000 systems, servers, and mobile devices. The assault disrupted manufacturing, order processing, and shipments across the globe. Hospital systems in Maryland were also affected, with healthcare providers forced to suspend connections to critical diagnostic tools.

The Stryker breach underscores a troubling pattern: private-sector companies, not just military installations or government agencies, are now primary targets of state-sponsored cyber operations. What was once a battlefield reserved for intelligence agencies and defense contractors has expanded to include hospitals, energy providers, data centres, and Fortune 500 corporations.

The Regulation Gap: Why Defenders Are Falling Behind

Rubrik CEO Bipul Sinha recently drew attention to a fundamental imbalance that is tipping the scales in favour of attackers. In a Fox Business interview, Sinha pointed out that cybercriminals and nation-state hackers face no regulatory constraints. They do not file compliance reports, wait for approval from oversight boards, or limit their use of emerging technologies. They simply adopt whatever tool gives them the greatest advantage and deploy it immediately.

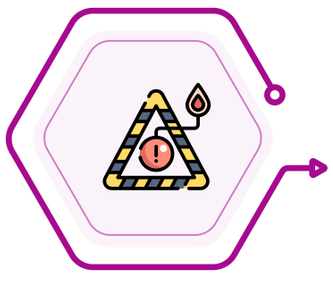
Corporate defenders, by contrast, operate within a dense web of legal and regulatory requirements. From data privacy laws and industry-specific compliance standards to emerging artificial intelligence governance frameworks, businesses must navigate a maze of obligations before implementing new security measures. This creates what Sinha describes as a speed gap. While enterprises spend months evaluating, testing, and gaining approval for AI-driven security tools, their adversaries are already weaponising the same technologies with no oversight whatsoever.



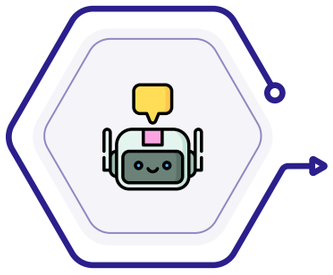
The result is a deeply asymmetric contest. Attackers iterate rapidly, experiment freely, and bear no consequences for failure. Defenders must be perfect every single time while following rules their opponents have never heard of and certainly do not respect.

The Agentic AI Threat No One Is Ready For

Perhaps the most alarming dimension of this evolving threat landscape involves the rise of agentic AI. These are autonomous software agents capable of executing complex tasks without continuous human oversight. In the corporate world, agentic AI promises to streamline operations, automate routine processes, and accelerate decision-making. In the hands of malicious actors, however, the same technology becomes a devastating weapon.



Sinha issued a stark warning about this emerging risk. If AI agents embedded within an organisation are compromised, a hostile actor operating from anywhere in the world could effectively take the reins of that business. Imagine a scenario in which an attacker sitting in Pyongyang gains control of automated procurement systems, financial workflows, or logistics platforms. The damage would extend far beyond data theft; it would amount to remote operational hijacking.



This is not a hypothetical concern. As businesses race to integrate AI agents into core operations, they are simultaneously expanding their attack surface in ways that traditional cybersecurity frameworks were never designed to address. The same features that make agentic AI so powerful for productivity, namely autonomy, broad system access, and decision-making authority, are precisely the features that make a compromised agent catastrophic.

Assume Breach: The New Corporate Mantra

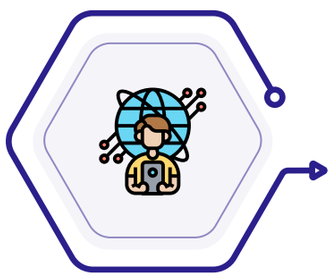
The mindset within boardrooms and security operations centres is shifting rapidly. According to Sinha, the dominant strategy among Rubrik's clients and prospective customers has become "assume breach." Rather than investing exclusively in perimeter defences that may eventually fail, organisations are channelling resources into detection, response, and recovery. The goal is not to prevent every intrusion but to ensure that when one inevitably occurs, the business can continue operating.

This philosophy is gaining momentum for good reason. The Stryker attack demonstrated that even a well-resourced multinational can be brought to its knees within hours. Companies worldwide are now asking urgent questions about their own resilience. How quickly can they detect an intrusion? How effectively can they isolate compromised systems? How soon can they restore operations and protect critical data?

Levelling the Playing Field

Closing the gap between attackers and defenders will require more than better software. It demands a fundamental rethinking of how governments, regulators, and private-sector leaders approach cybersecurity. Regulation must evolve to become an enabler of rapid defence rather than a bottleneck. Compliance frameworks need to accommodate the speed at which threats emerge and the urgency with which defenders must respond.

At the same time, the cybersecurity industry must put AI-powered tools directly into the hands of defenders, equipping them with the same technological advantages that adversaries already exploit. This means investing heavily in AI-driven threat detection, automated incident response, and intelligent recovery systems that can operate at machine speed.



The stakes could not be higher. The line between physical conflict and digital warfare has dissolved entirely. Every company with an internet connection is now a potential casualty of geopolitical disputes fought in cyberspace. The question is no longer whether businesses will be targeted but whether they will be prepared when that moment arrives.