THE CYBER DEFENSE REVIEW

The Cyber Defense Review is an open-access, peer-reviewed, scholarly journal that serves as a forum for current and emerging research on cyber operations. Its focus is on strategy, operations, tactics, history, ethics, law, and policy in the cyber domain.

The Cyber Defense Review positions itself as a leading venue for interdisciplinary work at the intersection of cyber and defense, welcoming contributions from the military, industry, professional, and academic communities.

The journal is committed to publishing original, previously unpublished, and intellectually rigorous research that advances the body of knowledge in this rapidly evolving field. We invite timely and relevant submissions that reflect both theoretical insight and practical application, with the goal of informing cyber-related decision-making, operations, and scholarship.

The Cyber Defense Review (ISSN 2474-2120) is published quarterly by West Point Press (https://westpointpress.com) and hosted by the Army Cyber Institute (https://cyber.army.mil).

THE ARMY CYBER INSTITUTE AT WEST POINT
·2012·

VOLUME 10 ◆ NUMBER 1 2025

THE CYBER DEFENSE REVIEW

The Battlefield is not 'Over There' – It is Here, 24/7
Lieutenant General Jeth B. Rey

A Conversation with the U.S. Army Chief Information Officer
Mr. Leonel Garciga,
interviewed by Deborah S. Karagosian

The Sword of Damocles: A Cybersecurity Paradigm Shift for the Defense of Critical Infrastructure
Scott C. Fogarty

Southeast Asia: Where Facebook is the Internet
Cadet Brandon Tran

Toward Clarity in Cyber's "Fog of Law"
Prof. Scott Sullivan

Lights Out: What Hurricanes Reveal about Cyberattacks and Blackouts
Tom Johansmeyer

Fighting Through Disruption: Reframing Cyber Resilience for Power Projection and Strategic Credibility
Dr. Karen Guttieri

INTRODUCTION
Forging the Future of Cyber Defense in an Era of Change and Uncertainty — *Prof. Robert Barnsby*

ARMY CYBER INSTITUTE ◆ WEST POINT PRESS

THE CYBER DEFENSE REVIEW
2025, VOL. 10, NO. 1, 29-39
https://doi.org/10.55682/cdr/kpwx-q1q1

PROFESSIONAL COMMENTARY

The Sword of Damocles: A Cybersecurity Paradigm Shift for the Defense of Critical Infrastructure

Scott C. Fogarty

Ridgeback Network Defense, Baltimore, MD, USA

The decentralized nature of U.S. critical infrastructure, while an engine and source of enormous societal wealth, creates significant vulnerabilities. Systems and their defenders are unknowingly operating underneath a modern Sword of Damocles—a constant and catastrophic threat of disruption from sophisticated and persistent adversaries. Drawing a parallel to the defensive failures of the October 7th Attacks, this article demonstrates how current cybersecurity strategies, heavily reliant on probabilistic, detect-and-respond tools, have proven insufficient to secure the complex Operational Technology (OT) systems and vast supply chains at the core of this infrastructure. This article argues that the fundamental asymmetry between attacker and defender can only be redressed by a new defensive paradigm. By integrating scalable, deterministic, and fact-based security methods with existing tools, defenders can enable automated, offense-for-defense capabilities. This approach, grounded in game theory, is the key to imposing tangible costs on adversaries in real time, finally allowing defenders to step out from under the sword and instead wield it.

Keywords: cybersecurity, critical infrastructure, operating technology, offense-for-defense, deterministic security, probabilistic security.

Disclaimer: *The views expressed in this work are those of the author(s) and do not reflect the official policy or position of the United States Military Academy, the Department of the Army, or the Department of Defense.*

Corresponding author: scott@ridgebacknet.com

Scott C. Fogarty is the CEO of Ridgeback Network Defense Incorporated. Scott leads Ridgeback with its founder and inventor, Thomas Phillips, a 25-year veteran of the U.S. Intelligence Community. Together, they build and deploy tools using a range of techniques that autonomously engage, disrupt, and impair attackers during exploitation Before Ridgeback, Scott led and founded media, information, and technology companies as CEO and was responsible for $1.5 billion in information industry Private Equity and Venture Capital investments. He earned a bachelor's degree from Harvard University and an MBA from Columbia University.

INTRODUCTION

More than our nation's isolation by two massive oceans that have protected us since its birth, America's greatest gift to its citizens is our constitutional republic – the system of government designed by our forebears to preserve individual freedom. These rights have underpinned the greatest system of free enterprise ever, delivering unprecedented levels of innovation, social progress, and wealth creation. In today's tech-connected world, however, our freedoms and the thriving economy they have created are vulnerable and exposed. The fragmented control over digitally powered critical infrastructure places key systems in the hands of tens of thousands of independent, self-directed entities. The same freedoms that foster innovation also generate countless vulnerabilities in cyberspace, where oceans no longer shield us.

The Sword of Damocles is a helpful anecdote to understand the nature of today's cybersecurity threat in critical infrastructure.

> When King Dionysius let Damocles trade places with him so he could experience the power, privilege, and wealth that Damocles enviously yearned for, Dionysius suspended a sword by a single strand of horsehair over his head to represent the constant threats that come with such power.

Similarly, the critical infrastructure that enables our way of life and the conduct of business in civilian, municipal, and military systems is quietly held at risk by adversaries unwilling to relinquish their advantageous positioning and power.

In a May 7, 2025, article titled 'Companies Want the Government to Go After Hackers. Washington Might be Willing,' the *Wall Street Journal* reported that a "relative lack of consequences for cyberattacks emboldens cybercriminals and nation state-backed hackers" and argues that "the situation won't improve unless Washington's attitude toward offensive operations changes" (Rundle 2005). Hoping the federal government will address the current situation is understandable. To do so, it is necessary to consider whether methods exist to tackle the challenge of securing critical infrastructure systems which enable participants and their supply chains to turn the tables on advantageously positioned adversaries. This article outlines the conditions and obstacles involved and suggests techniques available to critical infrastructure operators to impose costs on cyber adversaries in real time—*during exploitation attempts*—to confront these challenges directly.

A CAUTIONARY ANALOGY: OCTOBER 7 ATTACKS

While the October 7 attack on the Israeli Gaza envelope was clearly not a cyber attack, the defensive measures implemented by the Israeli Defense Forces (IDF) and the effectiveness of Hamas's tactics offer useful parallels for cybersecurity practices used to protect networks of all types and sizes—military, government, and private organizations, across both Information Technology (IT) and OT systems. The various security gaps exploited in the Hamas attack on Israeli citizens elucidate the inherent limits of a cybersecurity strategy that relies principally on surveillance and detection.

The main techniques used by the IDF to defend against attack were, first, enclosing Gaza with walls around its entire perimeter, and second, establishing an extensive network of surveillance, monitoring, and detection to raise alerts for threats. This included ground sensors, cameras, and radar. The strategy was designed to prevent direct attacks and to closely monitor potential enemy actions through information gathering or, more simply, to block and detect them.

How did Hamas wreak its harm so thoroughly? Like any capable adversary, their tactics drew on a proficient understanding of the capabilities deployed against them (Carchidi 2023). Planners employed three key methods to counter the defensive measures effectively. First, they shot out camera lenses and dropped drone-borne grenades on data collection points to degrade Israel's defensive information-gathering apparatus (Gosselin-Malo 2023). Next, they staged a singularly impressive feint by firing thousands of rockets into Israel to challenge air defenses (Granados et al. 2023). This provided a distraction from Hamas's main intent, which was to breach perimeter walls using methods that defensive systems were not tuned to detect. Although the IDF deemed paragliders and mopeds too small or slow to present serious threats (Carchidi 2023), Hamas used them to cross into Israel at as many as 30 breach points (Yarhi-Milo and Naftali 2023).

Following the heinous attack, analysts and the press were quick to criticize Israel for what they termed an "over-reliance on technology" (Carchidi 2023) of a nation with a "military tech fetish." (Gady 2023). Regardless of the specific interpretation, the core failure was that the right information did not reach the right commanders at the right time for a decisive response. In military terms, the OODA (Observe, Orient, Decide, Act) loops were broken, and the response came too late. This glaring paradox of a high-tech system failing so completely left one journalist to flatly question "how surprise was still possible in the AI [artificial intelligence] era." (App 2023)

There are parallels between these circumvented defenses and modern cybersecurity issues in critical infrastructure. Although cyber attacks occur on cyber terrain in different environments employing sophisticated technical methods, they share important features. In critical infrastructure, as adversaries approach target OT devices, they must navigate through increasingly obscure and outdated systems that are often beyond the reach of ‘detect and respond’ tools. Israel's delay in responding appropriately, possibly due to an overconfidence in its surveillance systems, offers a vital lesson.

> By depending on detection alone, the cyber defender unwittingly places themselves in the tenuous position of Damocles, enjoying an illusory sense of security while subject to the whim of Dionysius, who maintains power and control by being able to sever the thread at will.

SECURITY IMPLICATIONS OF DATA SCIENCE INNOVATION

Over the past 40 years, innovators have advanced cybersecurity tools and techniques from basic firewall and antivirus solutions to increasingly sophisticated and intelligent capabilities. Although there has been considerable innovation, most new tools are still incremental improvements rather than revolutionary leaps in capability. Across the entire range of cybersecurity solutions, approaches mainly focus on two core functions: *blocking measures* (walls) and *monitoring techniques* (detection), showing that the overall strategy has not evolved significantly. Essentially, current cyber defense postures are not much different from that of Gaza: they rely heavily on systems and processes that determined adversaries can circumvent.

AI's growing role in cybersecurity involves analyzing system telemetry and log data at a scale that is intractable for human analysts to handle. Using machine learning techniques for anomaly detection, pattern recognition, and threat classification, these systems identify statistically significant deviations from normal behavior. The outputs of these models are inherently probabilistic, providing a statistical inference that a given event warrants investigation, rather than a deterministic confirmation of fact. Crucially, this analysis is reactive, as it assesses system behavior that has, by definition, already occurred. In such inferences, there is no absolute veracity, the condition of being truthful or factual. The alert is a *maybe*, rather than a definitive *yes* or *no.* This paradigm results in security architectures attempting to analyze near-infinite data streams while defenders outsource critical judgments about the nature of events to automated systems that can only infer, not know, if a behavior is hostile.

Worse, when an adversary is in the mix, analytical AI solutions expand the attack surface and introduce new and significant risks. Reflecting this, ISACA, the global association of cybersecurity professionals, has warned that “attackers will leverage AI to craft highly sophisticated cyber threats,” affecting players across the supply chains and accelerating risks to critical infrastructure (ISACA 2025). This warning is particularly relevant because probabilistic tools themselves are vulnerable to the same types of deception and misdirection used in physical warfare. When statistics form the basis for detection, what happens if an adversary degrades AI models through data poisoning, bypasses them with novel techniques, or simply impedes the collection of system telemetry? What happens when a diversion is staged to draw defenders' attention from the primary attack vector? Or when an adversary leverages the same AI capabilities for offensive operations that are being used for defense? In the cyber domain, these tactics are equivalent to shooting out camera lenses, launching distractive barrages, and deploying penetration techniques that escape detection.

The Gaza example also highlights a second, equally important concern with using detection as a security foundation: the critical relationship between detection and response. The primary purpose of any detection capability is to enable swift and decisive defensive action. A key insight from this conflict is that monitoring and detection have limited value if they are not paired with a timely, effective response. On October 7th, there was evidence of two distinct failures: (1) adversaries manipulated detection systems, and (2) those systems failed to trigger the necessary and timely response. This mirrors a core challenge in cybersecurity, where incident response is inherently a rearguard action, often occurring too late to prevent impact. The speed of automated, AI-driven exploitation techniques compounds this issue, demanding automated defenses that can act without the latency introduced by inferential analysis.

Like Damocles, the sum of these innovations leaves the defender in a precarious and paradoxical state. They are surrounded by an immense feast of data and a celebration of sophisticated, AI-driven tools that provide a powerful illusion of security. But true initiative and the power to inflict the decisive blow remain squarely in the hands of the adversary.

> Upon noticing the sword that Dionysius so precariously hung over his head, Damocles immediately stopped celebrating the benefits of the wealth and privilege he enviously yearned for. King Dionysius was still in control. The presence of the sword alone made Damocles go mad, desperately begging Dionysius to let him go.

WHAT DOES THE RESEARCH SHOW?

Over the past five years, total annual spending on security tools more than doubled, increasing by over $100 billion to address the cybersecurity challenge (Borgeaud 2024). Notably, this period also saw the widespread adoption of increasingly sophisticated AI-driven monitoring and detection solutions. This doubling of resources, however, yielded disappointing results. According to IBM's 2024 *Cost of a Data Breach Report*, internal security systems and teams successfully detected breaches only 40% of the time (IBM 2024). The remaining compromises were disclosed either by a benign third party or by the attackers themselves during a ransom demand. This poor success rate raises a critical question about security strategy:

in what other domain would a strategy that fails more often than it succeeds be considered acceptable, especially given such high stakes?

Another key security objective following a compromise is limiting adversary dwell time—the period an intruder remains active in a system. Some security providers promote the notion that tools should detect, identify, and remediate compromises in 1-minute, 10-minute, and 60-minute timeframes, respectively. Unfortunately, reality falls far short. According to IBM, even as spending on security doubled—with a growing proportion dedicated to AI-based detection—adversary dwell time *increased* from 257 days five years ago to 277 days in 2023 (IBM 2023). Nine months is a long time for invisible, questionably-affiliated agents to have access to critical systems and networks without being detected.

Underscoring these failures, the technology research and advisory firm Gartner published a piece titled 'Stop Performing Cybersecurity Theater: It is No Longer Scaling'. The article argues that much of current practice gives only the appearance of security, stating, "Cybersecurity theater refers to actions that purport to reduce risk, without actually doing so... The size and complexity of the digital asset base is now so significant that cybersecurity leaders can't keep up with the demand to *pretend to protect* everything, let alone do so." (Heiser 2023)

These security gaps are particularly acute for the behavior of systems in OT enclaves. The industry's preoccupation with post-breach payload analysis is a poor fit for OT, where the focus should be on the attack sequence *before* a payload is deployed. Furthermore, common IT security techniques like deep packet inspection—which is central to many anomaly detection models—cannot be implemented on OT devices that lack the resources to host security agents. This approach is simply not viable for embedded systems that manage traffic lights, oil pipelines, water distribution, and power plants. This situation necessitates a re-evaluation of security frameworks toward verifiable standards that can proactively counter attacks, not just identify them after the fact.

> It's impossible for cyber defenders to lethally wield their swords over the heads of invisible adversaries if their defensive strategy is overly invested in passively observing the wrong things. King Dionysius knew exactly how and why the sword would quickly put Damocles back into his place.

THE CHALLENGE OF SECURING CRITICAL INFRASTRUCTURE

Securing critical infrastructure effectively is a complex undertaking. While sources of vulnerability are innumerable, the challenge can be understood through three high-level, interconnected themes.

- **Fragmented Ownership and Interconnected Systems:** Critical infrastructure in the U.S. is not a monolithic entity, but rather a network of independent organizations operating based on economic self-interest. This distributed ownership model results in inconsistent security standards and postures across the ecosystem. In such an environment, a single compromise can cascade through interconnected systems, yet no central command authority exists to enforce uniform security. This lack of centralized control is fundamental to the value generated by a free market. Still, it also creates an inherent, systemic security challenge that policy mandates alone cannot solve.

- **Heterogeneous and Legacy Systems:** Critical infrastructure consists of technologies bound together from different eras of invention. Tools from previous human generations are spliced together with devices of very recent vintage. These components were rarely designed with security in mind, yet they remain critical to operations. The proliferation of modern Internet of Things (IoT) devices has increased automation, but it has also ballooned the digital attack surface. This patchwork of disparate technologies, with varying security baselines, presents a thorny defensive challenge.
- **Complex and Varied Supply Chain:** Critical infrastructure functions rely on vast supply chains composed of numerous large and small entities and service providers. The modern emphasis on just-in-time logistics introduces risk at every node, as the disruption of only one minor link can cascade, potentially shutting down or stalling entire systems. Many smaller suppliers lack the wherewithal or the workforce to adopt best-in-class security measures. These less-secure entities often then become critical linchpins, the *weakest links* in the entire infrastructure.

Collectively, these three challenges severely limit visibility into system operations, both at the individual network level and across the entire critical infrastructure ecosystem.

THE DETERMINISTIC NATURE OF OT SYSTEMS

A potential answer to these challenges lies in the nature of OT itself. Unlike IT systems, OT is engineered to perform highly specific, well-defined functions within narrow operational parameters. Any deviation from this expected behavior is therefore a significant concern for both system reliability and security. This deterministic, state-based nature of OT is fundamentally at odds with the probabilistic, inference-based models common in IT security surveillance. In essence, OT systems are binary: they either operate as intended, or they do not. This intrinsic property offers a powerful insight for developing new and more effective security methodologies.

In an OT environment, control over an individual device is binary and zero-sum. If an adversary can write instructions to it, execute code on it, or influence its operation, they own it—you do not. The outcome is black-or-white. This fundamental principle means that failing to identify and cauterize the spread of an adversary's control inevitably leads to ceding system function and amplifying any resulting damage.

Probabilistic tools, by their nature, are imprecise. They deliver statistical inferences about the likelihood of abnormal behavior, not confirmed facts. Furthermore, these inferences often originate from opaque *black box* algorithms, making it difficult or impossible to audit the basis for an alert. In sharp contrast, deterministic approaches are fact-based, responding exclusively to verified conditions. They act only on data with absolute veracity, not on statistical probabilities.

Deterministic approaches rely upon the actual, fact-based behavior of a system as a direct trigger for action. This enables three key advantages: (1) conditions are observed and acted upon in real time; (2) responses can be automated to occur concurrently with the behavior, not after it; and (3) the response can be interactive, autonomously impairing an offender's ability to achieve their objectives.

When these fact-based, deterministic methods are paired with probabilistic AI, their benefits are compounded. Their combined effect creates: (1) reliable, constant confirmation that systems do no more or no less than what is expected; (2) higher-fidelity alerts from inferential analysis; and (3) a unique capability to meet automated attacks with automated counter-engagement in real time. By integrating these complementary methods, defenders gain a critical advantage.

A key operational benefit of deterministic approaches is their efficiency. They do not need to ingest and process enormous volumes of data, nor do they require instrumentation on every device. This makes them ideal for complex industrial environments, such as those consisting of Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) devices, where universal agent deployment is often impossible. As they do not rely on vast data lakes for statistical learning, they require minimal technical and workforce resources to deploy and manage.

Instead of implementing advanced tools to perform costly content inspection, these systems should focus on meta-evidence of system operations; observing which devices are on the network, how they interact, and whether those interactions are consistent with the intended system design. This lightweight approach is highly scalable, working equally well in both small and large network environments. Consequently, it is uniquely suited for universal implementation across diverse OT systems, including those at the smallest supply chain vendors.

WIELDING THE LETHAL SWORD OF DEFENSE

The fundamental asymmetry between cyber attackers and defenders cannot be redressed as long as resources are allocated to reactive *detect-and-respond* strategies. There is no winning by watching; this passive posture ensures the asymmetry will continue to favor the attacker. The strategic framework describing this dynamic was delivered decades ago by Nobel Prize winner John Nash in his 1951 thesis on game theory, 'Non-Cooperative Games'. In the zero-sum game he described, one player's gain comes directly at the expense of the other (Nash 1951).

In this model, each player chooses a strategy to optimize their outcome based on the opponent's likely response. An *equilibrium* is reached when neither player can gain an advantage by unilaterally changing their strategy (Nash 1951). In cybersecurity, a defensive strategy based solely on observation can never establish a stable equilibrium, because the attacker, facing no significant cost or penalty, will always find it advantageous to attack (or at a minimum remain concealed to retain the option to attack). To achieve a favorable outcome, a defender must move beyond passive surveillance and impose a tangible cost on the adversary. This is the only action that fundamentally alters the strategic dynamic in the defender's favor.

A novel technique based on monitoring unused IP (Internet Protocol) address space serves as an example of a deterministic capability that aligns with Nash's game theory. Every network allocates a range of IP addresses for devices to use. In a typical industry standard home network provisioned by a major broadband provider, for example, out of 254 available addresses, perhaps only 30 are in use by active devices. This leaves over 200 unassigned IP addresses, creating a digital *dark space.* All networks, from small home setups to large enterprise systems with millions of addresses, share this characteristic of having unused address space.

Any attempt by a legitimate device on a network to communicate with an unassigned *dark space* IP address is, by definition, a definitive indicator of illicit activity. This behavior is a hallmark of two primary threats: an intruder performing reconnaissance to map the network for an attack, or automated malware attempting to propagate by searching for new hosts to infect.

Because this observation is fact-based—possessing absolute veracity—it enables an immediate and automated response that occurs in conjunction with the actual condition or hostile action, not after it. This security measure matches an observation which has veracity – factual truth – with counter-engagement. The response can freeze the improper activity before it leads to harm. This capability introduces a true overwatch for cyber defense, analogous to the military tactic where one unit is positioned to protect another by immediately engaging threats when the protected element becomes vulnerable or falls under attack. In technical terms, this deterministic approach is equivalent to automating a *Man-in-the-Middle*, or perhaps a *Defender-in-the-Middle,* posture at scale. It effectively places a digital minefield between adversaries and their targets, allowing defenders to get off the reactive back foot and impose immediate costs. This shift from passive analysis to active, real-time offense-for-defense counter-engagement is key to changing the defensive paradigm.

> The swords we place over the heads of adversaries must present a visible, definitive, and costly threat that counters the advantage they seek and far outweighs the benefits they gain from being positioned in our systems.

CONCLUSION

This strategic shift transforms the defensive cybersecurity paradigm into a true Sword of Damocles over the heads of attackers. No longer a passive observer, the defender now wields a real and ever-present threat. The adversary must operate knowing the defensive response is not a probabilistic *maybe* but a deterministic certainty, held only by the single, fragile thread of the attacker's own behavioral choices. One wrong move—one attempt to touch the digital *dark space*—and the sword falls, not just ending the intrusion but imposing a real, automated cost. This is how the equilibrium of the game is finally changed in the defender's favor.

There are easy, lightweight techniques that are especially valuable to harden security in OT enclaves. Deterministic and fact-based approaches that limit their attention to (1) the universe of devices connected to systems and (2) the evidence of signals occurring between them (but not their content) provide the insights needed for understanding system behavior. By shifting focus away from inspecting and analyzing data packets to classify behavior, fact-based solutions can operate in real time while introducing offensive techniques that interdict, impair, and deter attacks. This offense-for-defense response has the effect of locking the process and freezing the connection open on the offending device so that it cannot lead to harm.

Because these methods focus on operational metadata rather than subjective analysis, they are highly scalable and efficient. This makes it practicable to deploy them universally across critical infrastructure, for any type of vendor or service provider, and throughout complex supply chains, even for smaller entities with limited resources. Detection-based solutions are importantly enhanced by the addition of complementary, offensively-oriented, and deterministic capabilities to the defensive posture. Neither alone can work as effectively as the two in concert. With the stakes for our security so high, implementing deterministic solutions alongside probabilistic ones supercharges our ability to achieve critical security goals within the context of existing investments in products and skills. Rather than replacing existing security investments, this fact-based approach complements and enhances them, creating a formidable, layered defense. A strategy of active, automated deterrence finally puts a real sword in the defender's hand.

> It is time for cyber defenders to step out from underneath the Sword of Damocles and instead wield it. We must transform our defense of critical infrastructure from an ineffective passive shield into an active, reliable, fact-based weapon that imposes immediate and direct costs on our adversaries.

REFERENCES

App, Peter. 2023. “Hamas Assault on Israel shows Surprise Still Possible in AI Era.” *Reuters*, October 9. https://www.reuters.com/technology/hamas-assault-israel-shows-surprise-still-possible-ai-era-peter-apps-2023-10-09/.

Borgeaud, Alexandra. 2024. “Spending on Cybersecurity Worldwide from 2017 to 2024.” *Statista*, June 18. https://www.statista.com/statistics/991304/worldwide-cybersecurity-spending/.

Carchidi, Vincent. 2023. “The October 7 Hamas Attack: An Israeli Overreliance on Technology?” *Middle East Institute*, October 23. https://mei.edu/publications/october-7-hamas-attack-israeli-overreliance-technology.

Gady, Franz-Stefan. 2023. “Israel’s Military Tech Fetish is a Failed Strategy.” *Foreign Policy*, October 26. https://foreignpolicy.com/2023/10/26/israel-hamas-gaza-military-idf-technology-surveillance-fence-strategy-ground-war/.

Gosselin-Malo, Elisabeth. 2023. “Hamas Drones Helped Catch Israel Off Guard, Experts Say.” *C4ISRNET*, October 18. https://www.c4isrnet.com/global/mideast-africa/2023/10/18/hamas-drones-helped-catch-israel-off-guard-experts-say.

Granados, Samuel, Ruby Mellen, Lauren Tierney, Artur Galocha, Cate Brown, and Aaron Steckelberg. 2023. “How Hamas Breached Israel’s ‘Iron Wall’.” *The Washington Post*, October 10. https://www.washingtonpost.com/world/2023/10/10/how-hamas-entered-israel/.

Heiser, Jay. 2023. “Stop Performing Cybersecurity Theater: It is No Longer Scaling,” *Gartner*, January 5. https://www.gartner.com/en/doc/779000-stop-performing-cybersecurity-theater.

IBM Security. 2024. “Cost of a Data Breach Report” *IBM Corporation*. https://cdn.table.media/assets/wp-content/uploads/2024/07/30132828/Cost-of-a-Data-Breach-Report-2024.pdf.

IBM Security. 2023. “Cost of a Data Breach Report” *IBM Corporation*. https://d110erj175o600.cloudfront.net/wp-content/uploads/2023/07/25111651/Cost-of-a-Data-Breach-Report-2023.pdf.

ISACA. 2025. “Cybersecurity in 2025: AI powered Threats, Supply Chain Vulnerabilities, and Regulatory Pressures Take Center Stage.” *ISACA*, February 20. https://www.isaca.org/about-us/newsroom/press-releases/2025/ai-powered-threats-supply-chain-vulnerabilities-and-regulatory-pressures-take-center-stage.

Nash, John. 1951. “Non-Cooperative Games.” *Annals of Mathematics* 54(2): 286-295. https://doi.org/10.2307/1969529.

Rundle, James. 2025. “Companies Want the Government to Go After Hackers. Washington Might be Willing.” *The Wall Street Journal,* May 7. https://www.wsj.com/articles/companies-want-the-government-to-go-after-hackers-washington-might-be-willing-93e0ba51.

Yarhi-Milo, Keren, and Tim Naftali. 2023. “The Lessons Israel Failed to Learn from the Yom Kippur War: Gathering the Right Intelligence Isn’t Always Enough.” *The Atlantic*, October 13. https://www.theatlantic.com/ideas/archive/2023/10/israel-yom-kippur-war-lessons-hamas/675627/.