social sciences

MDPI

Article

Techno-Digital Vulnerability and Intelligence Failures

Ehud Eiran

Department of International Relations, School of Political Science, University of Haifa, Haifa 3498838, Israel; eeiran@poli.haifa.ac.il

Abstract

Scholars and practitioners of international relations and security studies view technological capabilities in general, and digital ones in particular, as crucial to enhancing state power. Among other things, digital technologies sharpen intelligence, thus reducing the likelihood of strategic surprise by improving situational awareness and strengthening deterrence. Yet the empirical record of the early twenty-first century presents a paradox: states with highly advanced digital infrastructures remain vulnerable to unexpected strategic shocks, including intelligence failures. This article develops a conceptual framework, techno-digital vulnerability, that explains why digital superiority can paradoxically increase susceptibility to strategic surprise. Drawing on international relations theory, this article identifies four interrelated mechanisms: illusions of informational completeness; structural dependence on digital systems; hypervisibility of digitally open societies; and the systematic undervaluation of low-tech adversaries. The argument is illustrated through the case of Israel's failure to foresee the Hamas attack of 7 October 2023. The article concludes by outlining the implications for digitally advanced democracies and for the study of strategic surprise in IR.

Keywords: intelligence failure; Israel; techno-digital; Gaza; surprise attack; vulnerability

1. Introduction

The rapid digitalization of state infrastructures and military organizations has dramatically reshaped the foundations of national power. States increasingly rely on networks, sensors, platforms, AI-enabled analysis, and big-data architectures to manage borders, identify threats, and conduct military operations. Scholars and practitioners have embraced the assumption that digital superiority enhances security, and indeed a crucial building block of state power. Russian President, Vladimir Putin, famously stated in 2017 regarding artificial intelligence that "Whoever becomes the leader in this sphere will become the ruler of the world" (Allen 2017). It is a compelling narrative: more data, faster analysis, deeper surveillance, and continuous connectivity should produce earlier warning, more effective deterrence, and greater lethality. Within the realist tradition, technological advantage has long been treated as a multiplier of material capability (Mearsheimer 2001). Liberal and neoliberal scholarship similarly emphasizes the informational and institutional power generated by digital interdependence (Keohane and Nye 2012; Farrell and Newman 2019). In intelligence studies, the promise of improved collection and analysis through digital technology is taken seriously (Betts 2007; Zegart 2022).

Yet the last two decades have shown that digital superiority does not eliminate strategic surprise. The United States failed to anticipate the rapid collapse of the Afghan government in 2021 despite unmatched ISR (intelligence, surveillance, reconnaissance) capabilities. Russia misjudged Ukrainian resilience and Western resolve in 2022, despite extensive digital

Check for updates

Academic Editors: Azi Lev-On and Gal Yavetz

Received: 15 November 2025
Revised: 3 January 2026
Accepted: 9 January 2026
Published: 11 January 2026

Copyright: © 2026 by the author. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

monitoring. The COVID-19 pandemic surprised and challenged technologically sophisticated states that maintained elaborate global surveillance systems. Israel, a paradigmatic "start-up nation" with world-leading cyber units and an AI-integrated defense establishment, experienced a devastating intelligence failure on 7 October 2023.

These cases challenge the assumption that digital capability straightforwardly translates into greater security. They invite a rethinking of the relationship between technological advancement and strategic vulnerability. This article argues that the prevailing view of technology among security scholars and practitioners, especially the uncritical expectation that digital innovation naturally enhances power, obscures a more complex reality. Digital infrastructures introduce new forms of blindness, dependency, rigidity, and strategic exposure.

The central claim of this article is that the deeper a state's integration of digital technologies into intelligence, governance, and security practice, the more it becomes vulnerable to specific forms of strategic surprise generated by those same technologies.

This idea is captured in the concept of techno-digital vulnerability, a framework that illuminates how digital systems reshape the cognitive, organizational, and structural foundations of strategic assessment.

The article proceeds in five parts. First, it reviews the IR literature on technology and power, showing how dominant theoretical traditions often treat technological advancement as a stabilizing, capability-enhancing force. Second, it introduces the conceptual framework of techno-digital vulnerability, outlining four mechanisms by which digital superiority increases exposure to surprise. Third, it demonstrates the plausibility of the framework through empirical illustrations, drawing on Israel's failure to foresee the events of 7 October 2023. Fourth, it considers the broader implications for digitally advanced democracies, especially those that integrate AI and pervasive surveillance into their national security architectures. Finally, it outlines a research agenda for integrating digital systems into the study of strategic surprise and international security.

2. Technology, Power, and Perception in International Relations

The dominant paradigms of international relations scholarship generally treat technological sophistication as either a source of enhanced capability or as a structural feature of institutionalized interdependence. This section examines how major traditions conceptualize the relationship between technology and security, and why these approaches often overlook the vulnerabilities generated by digital systems.

2.1. Realism and the Accumulation of Power

Realist scholarship has traditionally conceptualized industrial capabilities, with technology at their heart, as a critical aspect of material power. The specific technology discussed in the literature changed over time, as technology itself changed. Initially, scholars focused on technology and science as enablers of heavy industries. By the 1990s, scholars paid growing attention to capabilities that stem from information technology. In his seminal text from 1948, *Politics Among Nations*, Morgenthau stated that: "the technology of modern warfare and communications has made the over-all development of heavy industries an indispensable element of national power. . ." (Morgenthau [1948] 1967, p. 113). These serve to create a strong economic base for a country, the foundation of the infrastructure needed in a total war, including "the quality of the highways, railroads, trucks, ships, airplanes" as well as "equipment and weapons of all kinds" (p. 113). As modes of production moved from heavy industry to information technology, also called by some, the "third industrial revolution" (Shchwab 2016, p. 7), so did the competition between states move to this realm. As economies moved to the fourth industrial revolution, the fusion of multiple connected

biological and information technologies "across the physical, digital, and biological domains" (Shchwab 2016, p. 7), global inter-state competition moved there as well. By 2025, scholars see the two great powers, the USA and China, engaged in a "tech war," in which the United States aims to maintain its technological supremacy while restricting China's access to critical technologies (Winkler 2025, p. 1).

Superior technologies enable superior coercive capability: more efficient militaries, more precise weapons, more effective intelligence collection. Realists argue that technology determines relative capabilities, alters the balance of power, and shapes deterrence outcomes (Mearsheimer 2001). Posen (2003) emphasizes how command of surveillance, navigation, and communications technologies helps major powers "command the commons," integrating global reconnaissance and precision-strike systems. Indeed, for Posen the key to the American "revolution in military affairs (RMA) has been the application of modern science and engineering—particularly in fields such as physics, chemistry, and information technology (IT)—to weapons design and use." For him, it was "the international dominance of the United States in these fields of science and technology that has made possible U.S. military dominance on the conventional battlefield" (125).

Within this tradition, technology is overwhelmingly treated as an enhancer of state capacity. Failures occur when states misinterpret data, allocate resources poorly, or fall behind technologically. The possibility that technological sophistication itself might create vulnerabilities receives far less attention. Even classical realists like Morgenthau acknowledged that overconfidence and misperception could accompany military power, but they did not systematically address the possibility that technical systems generate their own distortions.

2.2. Liberalism, Neoliberalism, and Digital Interdependence

Liberal and neoliberal traditions devote far more attention to information and interdependence. Keohane and Nye (2012) highlight how informational flows shape complex interdependence and the distribution of "soft" and "networked" power. More recent work, most notably, Farrell and Newman's (2019) concept of "weaponized interdependence", provides powerful insight into how states embedded in global digital infrastructures can leverage connectivity to monitor, coerce, or disrupt others. They offer a mixed picture. Technological advancement is primarily conceptualized as creating informational leverage, but also possible vulnerability. Similarly, studies of financial and supply-chain fragility acknowledge that deeply networked systems can fail catastrophically. Still, the vulnerability of intelligence and national security systems embedded in digital architectures remains generally underdeveloped.

2.3. Cyber Power, Ambiguity, and Fragility

Cybersecurity scholarship has made significant strides toward understanding how digital systems create new pathways for conflict and disruption. Scholars note that cyber capabilities often produce ambiguous, hard-to-detect effects (Lindsay 2013), that offensive advantages may be overstated (Gartzke 2013), and that digital infrastructures are inherently fragile (Slayton 2017). This literature highlights the paradox of power: digitally superior states may be more exposed to cascading failures or sophisticated cyber-attacks. However, the cyber literature has tended to focus on cyber offense and defense, not on the broader question of strategic surprise outside the cyber domain. It explains how hackers penetrate systems, but does not fully examine how reliance on those systems shapes misperception, decision-making, and warning.

2.4. Intelligence Studies: The Recognition of Cognitive Limits

Intelligence studies offer the closest theoretical insights into the issues addressed here. Scholars such as Betts (1978, 2007), Heuer (1999), Jervis (2010), and Bar-Joseph and

McDermott (2017) highlight that intelligence failures stem not from a lack of information but from cognitive rigidity, confirmation bias, organizational dysfunction, and politicization. Their insights remain highly relevant in the digital age: technology does not eliminate bias. Yet this literature also tends to treat technology as a tool that improves collection, timely dissemination, and possibly analysis. Most of the work, however, does not argue that information technology is a source of conceptual distortion in its own right. Analysts acknowledge that more data does not guarantee better interpretation, but the deeper structural and cultural consequences of digital integration have not been fully theorized.

2.5. Technological Superiority and the Paradox of Modern Military Power

Across military, policy, and organizational studies, a shared argument emerges that technological superiority constitutes a strategic double-edged sword rather than a linear source of advantage (Williams 2001; Serena and Clarke 2019). Advanced technologies reshape cognition and organizational behavior by fostering illusions of control, epistemic closure, and overconfidence, leading decision-makers to equate data abundance with understanding while discounting ambiguity, adversarial adaptation, and non-digital indicators (Bryant 2011; Peña 2024). This dynamic generates a paradox in which investments intended to enhance precision, speed, and dominance simultaneously create tightly coupled systems that are brittle, difficult to audit, and vulnerable to cascading failure, particularly in contested cyber and information environments (U.S. Government Accountability Office GAO 2018; Serena and Clarke 2019). Moreover, reliance on technological optimization often erodes redundancy and human expertise, reducing institutional resilience and adaptability under conditions of degradation or surprise (Bryant 2011; Plant CA 2023).

3. Toward a Conceptual Framework: Techno-Digital Vulnerability

This section develops a conceptual framework to explain why technologically advanced states remain susceptible to strategic surprise: techno-digital vulnerability. The core claim is that digital systems reconfigure the political and organizational environment in ways that generate illusion, dependency, exposure, and misrecognition. These dynamics are not epiphenomenal but intrinsic to the operation of digital infrastructures within bureaucratic systems.

3.1. Digital Systems as Producers of Illusion

Digital intelligence architectures routinely engender a cognitive and organizational illusion of epistemic completeness, projecting an image of seamless, real-time situational awareness. The massive proliferation of multi-spectral sensors, big data repositories, algorithmic filtering, and automated pattern-recognition suites reinforces the belief that the battlespace, as well as the political leadership that directs collective actions, has become fully transparent. This effect is a security-specific version of automation bias. Automation bias is the systematic tendency to over-rely on an automated aid's output and to reduce independent information search and verification, especially when the automation appears authoritative or when workload/time pressure is high. Automation bias could be a result of either commission or omission errors. The former is following wrong automated advice despite contrary evidence. Omission errors are cases of failing to act because the system did not flag something, leading to an assumption that if there is no alert or no information, there is also no problem. The actors use automated cues as a heuristic replacement for vigilant information seeking and processing (Parasuraman and Manzey 2010).

This effect is particularly pronounced in security establishments structurally dependent on SIGINT (Signal intelligence)-dominant collection strategies, integrated border-monitoring arrays, and persistent ISR platforms. Yet the vulnerability is not purely technical.

It is fundamentally epistemological and organizational: these systems cultivate illusions of omniscience, generating a false sense of closure that narrows interpretive bandwidth, crowds out dissenting analytic pathways, and entrenches a confirmation-biased threat-assessment equilibrium. Moreover, security officials, and especially intelligence officers, operate under conditions of significant workload (Heuer and Pherson 2015), which makes them even more susceptible to using heuristics such as reliance on technology, because "Information overload degrades judgment and increases reliance on heuristics, particularly under time pressure" (Eppler and Mengis 2004).

The result is a paradoxical decline in strategic warning capacity precisely as digital density increases.

3.2. Digital Systems as Dependency Structures

Once intelligence and security organizations integrate digital systems deeply into their daily routines, they may become structurally dependent on them. Analysts are trained to report data streams and may abandon the effort to deeply understand a foe. They might also tend not to question the systems that generate them. Under these conditions, other sources of information, such as deep tracking in a foe's culture, as well as HUMINT (Human intelligence), might be deprioritized, and decision-makers become habituated to real-time visibility, making system disruptions catastrophic.

3.3. Digital Societies as Hypervisible Targets

Modern societies, especially digitally open societies, produce enormous quantities of publicly accessible data through social media, civilian mapping, commercial satellite imagery, and digital bureaucratic interfaces. This creates unprecedented visibility for adversaries, especially those using OSINT (Open source intelligence) techniques.

3.4. Digital Cultures as Generators of Misrecognition

Finally, accelerated digital advancement often reinforces techno-nationalist imaginaries and narratives of civilizational or technological exceptionalism, producing a form of strategic hubris embedded in national identity discourse. Such ideational constructs diffuse into elite strategic culture, shaping political expectations, organizational standard operating procedures, and the epistemic priors that guide threat interpretation. In this cognitive environment, decision-makers and intelligence professionals become predisposed to asymmetric underestimation biases, systematically discounting the adaptive ingenuity of low-tech or resource-constrained adversaries. This hubristic framing narrows the perceived opportunity structure available to opponents and obscures potential pathways for low-signature innovation, deception, and doctrinal surprise. In turn, it encourages a false sense of digital dominance, attenuating strategic empathy and degrading anticipatory intelligence.

4. Techno-Digital Vulnerability in Practice: Digital Systems, Cognitive Bias, and Strategic Perception

If the first part of this article outlined the conceptual foundations of techno-digital vulnerability, the next step is to explore how this framework manifests in real political and organizational contexts. Digital infrastructures do not simply improve a state's intelligence capabilities; they also reshape how states perceive threats, how organizations interpret signals, and how policymakers understand their own power. This section deepens the analysis by examining three domains where the consequences of digital integration and techno-digital vulnerability are most evident: the cognitive domain, the organizational domain, and the geopolitical domain.

4.1. The Cognitive Domain: Digital Illusion and the Compression of Uncertainty

One of the most powerful effects of digital systems is their ability to compress uncertainty. High-resolution satellite imagery, persistent surveillance platforms, automated sensors, and AI-enhanced analytic tools appear to eliminate ambiguity. Political leaders and intelligence officials accustomed to such systems might begin to experience what can be called epistemic saturation: an overwhelming impression that the available information is not only abundant but comprehensive.

In such environments, the unknowns appear marginal. This is not simply a psychological bias; it is an emergent property of how digital systems integrate into everyday practices of intelligence work. Digital interfaces present information in clean, structured, and quantifiable formats. Error margins are hidden beneath layers of computation. The sheer volume of data implies exhaustive coverage. Digital architectures thus have a performative effect: they present themselves as complete, even when they are not.

The cognitive impact is profound. Strategic warning is fundamentally about interpreting ambiguous indicators. But digital systems tend to present data as discrete, reliable, sensor-generated facts rather than as fragments of a partially observed strategic environment. Analysts internalize the idea that if a threat were emerging, it would appear in the data. When the data is silent, analysts might infer that the strategic situation is stable, even when adversaries deliberately conceal their activities by avoiding detectable electronic signatures.

This process creates what Robert Jervis, in a different context, called "premature cognitive closure" (Jervis 2010). Digital architectures encourage the premature closure of interpretive possibilities by projecting an aura of completeness. Once an intelligence organization believes that its sensors can detect every relevant action, alternative scenarios, especially those involving deception, analog behavior, or low-tech operational methods, may appear unlikely, even irrational.

The result for intelligence analysts is a cognitive narrowing: an inability to imagine certain kinds of threat because the digital system that is presumed to reveal such threats does not display them. Theories of intelligence failure emphasize this dynamic in pre-digital contexts (Heuer 1999; Betts 2007), but digital systems intensify it dramatically.

4.2. The Organizational Domain: Digital Dependency and the Transformation of Intelligence Work

Beyond cognition lies a second domain: organizational dependency. Intelligence agencies are not simply repositories of analysts; they are complex bureaucratic systems whose routines are shaped by their tools. Over time, organizations that rely heavily on digital infrastructures internalize the assumption that those systems will always function as intended. Digital systems reconfigure the architecture of intelligence work in several ways.

First, they change the hierarchy of collection methods. SIGINT, IMINT (Imagery intelligence), and data-driven analysis tend to displace HUMINT, qualitative field reporting, and contextual interpretation. This is partly due to perceived objectivity: digital data is treated as more reliable, less biased, and inherently superior to human reporting. Analysts trained in such environments are incentivized to privilege what appears in the digital picture and to discount signals that rely on human interpretation.

Second, digital infrastructures generate new forms of organizational inertia. Because digital systems require continuity, standardization, and technical maintenance, intelligence routines become more rigid and less adaptable. Over time, organizations begin to rely on consistent patterns of data collection, consistent indicators, and automated alerts. The system teaches its users what to see and what to ignore.

Third, digital dependency erodes resilience. When digital infrastructures fail, whether due to system disruption, targeted attack, or adversarial deception, analysts and decision-

makers often lack the analog skills or institutional redundancy necessary to compensate. The more effective digital systems appear during normal operations, the more catastrophic their failure becomes during crises.

Thus, digital superiority generates an invisible but significant vulnerability: it reduces the adaptive capacity of intelligence organizations. Bureaucratic routines become optimized for the digital environment, not for uncertainty. When adversaries behave in ways that do not generate digital signatures, through analog communications, low-tech mobility, or deliberate deception, the organization struggles to compensate.

These organizational dynamics are not unique to any one state or intelligence community; they are structural features of digital transformation. As more intelligence organizations modernize, these vulnerabilities may spread across digitally advanced democracies.

4.3. The Geopolitical Domain: Digital Openness and the Strategic Exposure of Democracies

Digital technologies do not operate only inside intelligence agencies; they permeate society. Indeed, in information technologies, the causal arrow is at times the other way around, as intelligence agencies adopt civilian technologies for their needs (Katz 2020). Democracies that embrace digital openness, widespread social media use, public mapping services, transparent bureaucratic systems, and high levels of digital literacy produce vast quantities of information that adversaries can exploit. This is a structural asymmetry: open societies are more visible than closed ones.

This asymmetry has profound strategic implications. In the analog era, an adversary needed significant intelligence infrastructure to collect meaningful information on societal tensions, political movements, military mobilization, or logistical vulnerabilities. Today, much of that information is freely available. The digital state exposes its patterns of life to the world, including to hostile actors.

In authoritarian systems, by contrast, the state can minimize digital exposure by creating digital walls that separate it from the rest of the world, by censoring social media, restricting geolocation services, or nationalizing digital infrastructures. Authoritarian secrecy is not absolute, but it can reduce the volume and granularity of available information.

Digital openness redistributes visibility. It shifts who can observe what. Liberal democracies become transparent not only to their own citizens but to adversaries. This shift challenges long-standing assumptions about intelligence asymmetry. In many contexts, low-tech actors, insurgencies, and hybrid organizations may possess better visibility into the operational vulnerabilities of technologically advanced states than vice versa.

Digital openness, therefore, becomes a structural vulnerability in the international system. It creates what could be called informational asymmetry in reverse: the strong become visible, and the weak become less so.

5. Illustrating the Framework: Israel and the Strategic Surprise of 7 October 2023

This section illustrates the framework by examining how techno-digital vulnerability manifested in the Israeli failure to foresee the 7 October 2023 Hamas attack. This is not a full case study; it is an analytic illustration intended to show how the four mechanisms: illusion, dependency, hypervisibility, and misrecognition, played out in a real-world context. Israel is a useful illustration because it is among the most digitally integrated states in the world: society, armed forces, and the intelligence services all stress the importance of information technologies. Israeli intelligence doctrine has long emphasized persistent surveillance, rapid analysis, and operational responsiveness. In many ways, Israel represents the ideal type of a digitally empowered state. Yet on 7 October 2023, Hamas, a hybrid organization with limited resources relative to a state, successfully executed a multi-pronged, large-scale

surprise attack. The attack exploited weaknesses in Israeli early-warning systems, border defenses, and military mobilization. The scale of the failure was shocking precisely because of Israel's reputation for technological superiority.

5.1. Israel and Advanced Information Technology: Society, Armed Forces, and Intelligence Agencies

The Zionist movement gave technology a central role since its earliest days. Led by a small technocratic elite who spearheaded a settlement project in Ottoman-ruled Palestine starting in the late 19th century, Zionists "reproduced albeit on a far smaller scale, the activities of the technically-oriented elites in European society in the late 19th century" (Penslar 1991, p. 6).

The pre-state Jewish political entity, first under the Ottomans, but mostly under the British, prioritized scientific and technological education. The movement's instigator and first leader, Theodor Herzl, embedded his 1902 utopian book, *Old New Country*, with the centrality of science to the Zionist political project. The protagonist was trained as a scientist, and the futuristic state both advances the values of science and draws much of its success from applying it (Herzel 1902). The most dominant Zionist leader after Herzl, Chaim Weizmann, was a scientist who moved from Russia to the United Kingdom in the early 20th century to assume a position of a senior lecturer at the department of chemistry at the University of Manchester. Upon Israel's creation in 1948, Weizmann was elected as its first President (Reinharz and Golani 2024). The first academic institute to be created by this new wave of Zionist immigrants was the Technion, the Israeli Institute of Technology, which was envisioned in the early 20th century and launched in 1912, still under the Ottomans. By the early 21st century, it boasted a number of Nobel laureates and ranked in one survey as the leading global institution in digital education (Technion UK 2024b).

Once the Jewish political entity in Palestine transformed into an internationally recognized state, the focus of science and technology only intensified. The state's first Prime Minister, David Ben Gurion, declared in 1949 that the "revival of the nation of Israel, building a state out of ruins, developing our economy to be able to absorb millions of immigrants, and securing economic independence, is all conditional on the maximal development of science in Israel" (Ben Gurion 1949, p. 582). The reality of a military threat created a further incentive for investing in science and technology, as a way to balance the asymmetry in resources between the small Jewish state and the vast, hostile Arab world around it. The Israel Defense Forces created in 1948 a science corps, which later evolved into a national authority for weapon development (RAFAEL). The unit's first commander, bio-physicist Ephraim Katzir, and his brother, chemist Aharon Katzir, continued to advocate for the centrality of science in Israel (Katzir 1971). In a clear signal of the importance of their message, Ephraim Katzir was elected in 1973 as Israel's fourth President (Arnon et al. 2016). The Israeli state went on to invest from a rather early phase in technological research and development. By 2025, it was one of the top providers of such funding among OECD countries (Harris 2025).

As the global focus on technological innovation shifted toward information technologies, the Israeli state began directing its efforts to support the development of new products in this area as early as the 1970s. This was mostly achieved by grants to new companies, including capital injection in times of global crisis such as the one that affected the industry in 2008 (Cohen 2011). In assessing this policy, Breznitz concluded that "Israel's IT industry is an impressive success" (Breznitz 2007, p. 41). This success was further translated to a self-image and outwardly directed image of an innovative society and state to be dubbed the "start up nation" (Senor and Singer 2009).

The centrality of science and technology in society was, as noted, echoed by the defense establishment that saw in science and technology a force multiplier, and a possible balancer

against Arab numerical superiority. Freilich (2018) summarized this approach in Israel's defense posture, when he explained that the vision was that "Israel's more advanced operational technological capabilities would make it possible for the same number of aircraft to fly more sorties, for tanks to achieve a higher percentage of hits and for Israel's ground forces to conduct reward of greater mobility" (24–25). Indeed, the state created a set of institutions that supported the development of science for military purposes, and constructed a massive defense industry that by 2024 had become a leading element in Israeli exports with almost USD 15 billion in annual exports (Azulai 2025). On the other hand, as early as 2006, Meir Finkel, an Israeli general and thinker, warned against the "cult of technology" which may come at the expense of other aspects of military readiness, including doctrine, training, development of human resources, and supplies (Finkel 2006).

Within the defense establishment, the intelligence agencies are perhaps the most noted users of technology for collection, analysis, and dissemination. These, as I will show, are increasingly used for targeting. The process had its sources in the Israeli learning from the American wars in Iraq (1991) and Kosovo (1998–1999), when the ability to collect accurate data from multiple sensors and then use it for effective targeting was made evident (Amidror 2002). In the Israel Defense Intelligence (IDI), this revolution really took off in the 2010s, driven above all by the maturation and diffusion of advanced targeting technologies. Under Maj. Gen. Aviv Kochavi (2010–2014), the IDI restructured its doctrine and organizational interfaces around the accelerating convergence of ISR (Intelligence, Surveillance, and Reconnaissance), cyber, data-analytic, and precision-strike capabilities. The strategic turbulence following the Arab Spring, state collapse, and Iran's expanding regional reach undermined the centrality of conventional militaries and elevated hybrid adversaries embedded in civilian terrain. Yet what rendered this shift operationally meaningful was not so much the changing nature of threats as the emergence of technologies that enabled unprecedented levels of detection, identification, and rapid engagement (Eiran et al. 2025).

The IDI increasingly assessed that the likelihood of large-scale interstate war was diminishing, while prolonged sub-conventional competition was becoming the modal conflict environment. In this context, targeting became the core organizing function of the intelligence enterprise. Israel correspondingly expanded its investments in offensive and defensive cyber capabilities, automated data-processing systems, persistent surveillance platforms, and algorithmically enhanced fusion engines. Unit 8200 played a central role in these developments, particularly in operations that exploited digital vulnerabilities (e.g., the Stuxnet campaign against Iran in the first decade of the 21st century), while IDI focused on compressing the sensor-to-shooter cycle to near-real-time levels. Newly constructed digital architectures sought to produce what IDI officials described as continuous, cross-domain awareness, enabling rapid cueing of fires, pinpointed disruption of networks, and seamless transfer of intelligence to maneuver units (Eiran et al. 2025).

These innovations were institutionalized within the logic of the *Campaign Between Wars* (Mabam), which reconceptualized intelligence as an operational instrument rather than a predominantly strategic warning function. Mabam operationalizes a regime of persistent, low-visibility coercion aimed at degrading adversary capabilities and shaping escalation dynamics. Crucially, this approach depended on the ability to generate high-velocity targeting intelligence, enabling an ongoing cycle of detection, attribution, and calibrated strike. In this doctrinal environment, it was repositioned from a supplier of episodic assessments to a central node in a technologically enabled kill chain (Ortal 2021).

Senior IDI leadership made this shift explicit. In 2017, Maj. Gen. Herzi Halevi underscored that proliferating precision-strike systems and unmanned platforms, combined with adversaries' dispersed, cellular structures, necessitated embedding intelligence within combat formations far more deeply than before. Israel no longer faced a finite set of state

militaries but, in Halevi's words, "an endless number of individuals and organizations" capable of leveraging relatively cheap but operationally consequential technologies such as drones. Under these structural conditions, he argued, "intelligence becomes the compass for initiative, directing fire and maneuver. The real metric of a modern military is its ability to bring intelligence to the field and connect it to offensive and defensive action" (Halevi 2017).

This logic diffused across the intelligence community. In 2021, the deputy commander of Unit 8200 observed that the unit had shifted from "providing early warning for war" to "conducting offensive action daily," a shift only possible through the proliferation of digital targeting technologies (Limor 2021). That same year, the Research Department abandoned its 1990s warning-centric motto in favor of a new guiding principle, "knowledge, in context, for purpose", capturing the IDI's transition from anticipatory analysis to continuous, technology-driven targeting support (Eiran et al. 2025). It also created, in 2021, a new institute together with the Israeli authority for weapons development, Rafael, called Gazit, which was branded as a part of the "technological revolution" in IDI. It was committed to transforming intelligence analysis to a process based on "advanced technologies. . .using quantitative abilities, and developing new apps" (Israel Defense Intelligence (IDI) 2021). IDI and other intelligence agencies stressed AI-driven surveillance platforms (Technion UK 2024a), as more tactical intelligence units deployed sophisticated border-monitoring systems (Israel Trade Mission in Keniya 2022).

Taking a broad view, these were three separate but interconnected processes: an embrace of new technologies, which led to a greater focus on tactical and operational intelligence, and a weakening of the focus on strategic intelligence. The more the IDI could demonstrate its value as a participant in tactical and operational efforts, the less focus it gave to strategic intelligence. This, then, led to a delusion: the technology-based command of the tactical and operational sphere led the IDI leadership to believe that they also have command of the strategic realm, and that Israel's foes will be unable to carry out a significant change in their policies without data traces that Israel would pick up. These could either be information gathered at the strategic level, or a set of indicators on the tactical level, that will offer a cumulative picture of a change in policy, seen from the bottom up. The centrality of technology in this belief system led Israel to abandon the development of other sources that had traditionally provided information on the strategic level, most notably, human sources. Indeed, it was recently revealed that in the two decades prior to the 2023 Hamas attack, Israel had no senior human sources in the Gaza Strip (Eyal 2025).

As we will show in the following section, this belief led to massive failure.

5.2. The 7 October 2023 Surprise Attack and Israel's Intelligence Failure

In the morning of 7 October 2023, over a hundred Hamas squads breached the border fence separating Gaza from Israel and attacked military bases, civilian communities, and two nature parties. At the end of the day, almost 1200 Israelis were dead, and 251 dead and live Israelis were abducted to Gaza. The Israel Defense Force was able to retake and clear the occupied areas within 24–48 h. Shortly afterwards, it launched an attack on Gaza. The war expanded to include Hezbollah in Lebanon, the Houthis in Yemen, and then Iran. The war ended only in October 2025; by then, some 90,000 people were killed, mostly in Gaza, but also in Israel, Lebanon, Syria, Iraq, Yemen, and Iran.

Israeli intelligence failed completely in issuing a warning about the attack. The intelligence failure on 7 October was on all three levels: tactical, operational, and strategic. At the most proximate level, Israeli intelligence did not generate a tactical early warning, a narrow, time-sensitive alert that should precede an imminent attack, despite the presence of actionable indicators in the hours before the assault. Signals that ought to have triggered

rapid force posture adjustments were discounted or mischaracterized. Even after two late-night and pre-dawn consultations among senior military and intelligence officials, the system failed to translate ambiguous tactical cues into a concrete warning. The window for preemption consequently closed. There was also an operational intelligence failure. Years prior to the attack, the intelligence community possessed substantive insight into Hamas's campaign design, including the plan known in Israel as *Walls of Jericho*. Yet this information was not effectively diffused into the IDF's (Israel Defense Force) operational planning and force-employment frameworks. As a result, the Southern Command's defensive posture did not evolve in line with the adversary's emerging capabilities and doctrinal shift. This reflects a pathological combination that is familiar in the intelligence studies literature: organizational overconfidence, mirror-imaging, and the routinization of assumptions about the opponent's "learned" behavior, which altogether degraded the system's ability to adapt (Bob 2025).

The most far-reaching breakdown, however, was strategic. Strategic warning is intended to sensitize decision-makers to long-term shifts in an adversary's preferences, risk tolerance, and theory of victory, even when such shifts are imperfectly observable. Israeli intelligence failed to register Hamas's transition from episodic, calibrated rocket exchanges designed to preserve the movement's organizational survivability to a high-risk, high-payoff strategy predicated on a massed ground incursion by over a thousand fighters. This failure stemmed partly from Hamas' successful deception and operational security, but also from a broader analytic blind spot: the persistence of an outdated conceptual model of Hamas as a cost-averse actor seeking limited conflict. In effect, the strategic-level epistemic frame through which Israeli agencies interpreted Hamas became decoupled from the organization's evolving doctrine and intent (Siman-Tov and Guterman 2025).

Taken together, these three tiers of failure, tactical misinterpretation, operational misalignment, and strategic misdiagnosis illustrate the classic dynamics of intelligence surprise identified in the scholarly literature: cognitive rigidity, organizational fragmentation, and adversary deception converging to disable early warning at precisely the moment it is most needed. The following subsections analyze the four aspects of vulnerability that led to the intelligence failure.

5.3. Digital Illusion: The Failed Notion of Intelligence Dominance

Israeli intelligence believed that its surveillance systems provided deep penetration to all its foes in the region, including Hamas. Indeed, its organizing approach was defined as intelligence dominance (ID), which was to support intelligence-directed combat operations as the IDI's central mission. This came at the expense of trying to provide early warning (Eiran et al. 2025). In 2022, Chief of Staff Kochavi (earlier, the director of IDI) was proud to report in a public event that accurate information allows the IDI to know the exact content of each truck in a convoy that carried arms from Iraq to Syria. This, he said, coupled with the relevant munitions, represents "very advanced capabilities" (Maariv Staff 2022). Over time, this success created the belief that all regional foes, including Hamas, could not organize without producing detectable signals.

The digital architecture thus reinforced a misleading strategic conception. Intelligence organizations treat systems as sources of truth. When systems show stability, analysts often infer strategic stability, even when the silence reflects adversarial adaptation rather than genuine calm.

5.4. Digital Dependency and Systemic Paralysis

The second mechanism of organizational dependency became evident during the attack itself. Hamas neutralized parts of Israel's digital surveillance architecture early in

the operation. Drones destroyed communication towers and cameras; power lines were cut; and key nodes of the digital fence were disabled (Halabi 2023). The effect was not merely the loss of visibility; it was organizational paralysis. Units accustomed to real-time digital situational awareness lacked alternative methods to generate information. Manual reporting systems were slow. IDF investigations concluded that the "Headquarters' operations center was unable to understand the picture on the ground in the first few hours [of the attack]." There was even a difficulty in understanding the state of the subordinate command and control centers, especially the Gaza division (Zeitun 2025). Units on the ground and the air force struggled to communicate about the scale of the infiltration and to coordinate an effective response. The entire system, which is centralized, digital, and sensor-dependent, was unable to reconstitute visibility once its primary infrastructure collapsed. Digital dependency thus converted localized system failures into systemic breakdowns.

5.5. Hypervisibility and Adversarial Exploitation

Hamas exploited Israeli digital openness in several ways. Since Hamas's takeover of the Gaza Strip in 2007, the organization's overt intelligence-collection activity has become institutionalized, primarily through the Military Intelligence Department of the Izz al-Din al-Qassam Brigades. This activity relied heavily on Israel's digitally accessible open media environment, which provided the organization with extensive access to information on the IDF, the security establishment, Israeli politics, and Israeli society. Hamas developed a systematic apparatus for monitoring Israeli media, which included, among other things, regular publications. For example, since 2007, it has issued a weekly report entitled *Israeli Affairs*, which covered a wide range of civil and security issues in Israel. The report summarized key events, analyzed them, and concluded with an operational assessment for internal use.

Publications addressing the Israeli military included information on the IDF's structure, exercises, and new weapons systems. Information was gathered through print media, television, radio, and internet sites. Hamas also made use of video documentation of battles in Gaza released by the IDF to the media, such as footage from the July 2007 encounter with the Golani Brigade, to train its fighters in recognizing the dangers of Israeli aerial and thermal observation (Flamer 2024, pp. 59–79). Public social media also offered Hamas a window into discussions about political polarization and reservist protests. These provided visible cues about Israeli societal stress. Civilian drone videos circulating online revealed patterns of border patrol movement. Publicly accessible satellite imagery illustrated military infrastructure, terrain features, and even the internal makeup of bases that were later attacked (Ashkenazi 2025).

5.6. Hubris and Underestimating the Power of Low-Tech Creativity

Finally, Israeli political leaders and intelligence agencies overestimated their own capabilities and underestimated Hamas' capabilities, based on the gaps between the two societies in deployment and access to technology. Perhaps most famously, former Prime Minister Bennet described the Palestinian issue in 2013 as painful but manageable, like a "piece of shrapnel in the backside" (Schif 2024). In effect, he implied that the power differentials in favor of Israel will allow it to contain Palestinian national aspirations. Much of Bennet's worldview of Israeli power is based on its technological prowess, in part, as he is Israel's only Prime Minister who emerged from the technology sector (Maimon and Alony 2019).

Israel was under the impression that its technological advantage had blocked Hamas' ability to cross the border. Since at least 2014, Israel has seen the main threat from Gaza as cross-border tunnels. In the late 2010s, it embarked on a massive project of technology-

laden barriers, including sensors and underground walls that would neutralize their threat. In December 2021, the project, which had cost USD 1 billion, was completed and declared operational. The barrier, defined by the IDF as a "defensive system", was loaded with technology. It comprised a physical and technological underground barrier of 65KM, an above-ground fence rising more than six meters and integrated with systems designed to neutralize drones, aircraft, and other aerial platforms, as well as a naval barrier equipped with sensors for detecting maritime infiltrations and a remotely operated weapon system. Complementing these were a network of radars and cameras providing situational awareness and tunnel-detection capabilities, alongside command-and-control centers operating at the battalion, brigade, and division levels. Upon its completion, both the Minister of Defense and the military's Chief of Staff congratulated themselves by describing the barrier as "technological and creative", one that reflects an "outside the box thinking" (Israel Defense Force (IDF) 2021). When actual plans of an aboveground Hamas attack were intercepted, Israeli intelligence officials dismissed them as "empty bragging", not accepting that a technologically inferior foe might be able to overcome technologically advanced Israel (Eyal 2024). Digital superiority had created a strategic imaginary in which technologically inferior tactics by a technologically backwards foe appeared implausible. The ability of paragliders, bulldozers, and simple explosives to defeat sophisticated digital barriers was underestimated. Low-tech innovation was not integrated into strategic assessment, even when it was visible.

6. Findings: The Paradox of Digital Power

The Israeli illustration is not an anomaly. It underscores the broader theoretical point that digital power does not simply strengthen states; it reshapes vulnerability. The four mechanisms of techno-digital vulnerability operate independently but also reinforce each other. Digital systems create illusions of certainty. In this case, it is the Israeli illusion of intelligence dominance. Illusions generate cognitive rigidity and an inability to imagine that a less technological foe could innovate. The result is a paradox: states become less capable of interpreting threats precisely when they believe their digital infrastructures provide them with unprecedented control. The Israeli case illustrates this dynamic, but similar patterns appear in other contexts. The United States experienced a form of digital illusion in Afghanistan, where data-rich assessments failed to capture the fragility of political legitimacy. Russia experienced misrecognition when it misjudged the capacity of the Ukrainian state and the resolve of Western European actors. Democracies across Europe have experienced hypervisibility through targeted disinformation campaigns. The vulnerabilities identified here are therefore structural, not idiosyncratic.

7. Discussion

This article advances the existing literature on technological overreliance by moving beyond normative warnings and organizational critiques toward a systematic IR-level explanation of why digital superiority can generate strategic vulnerability. Whereas prior work emphasizes the paradoxes of technological dominance, cognitive overconfidence, and systemic brittleness in general terms, this article contributes a unifying conceptual framework, *techno-digital vulnerability*, that specifies the mechanisms through which digital systems reshape cognition, organization, and strategic interaction in ways that increase susceptibility to surprise.

By theorizing the four mechanisms of (1) illusion of informational completeness, (2) structural dependency, (3) societal hypervisibility, and (4) systematic undervaluation of low-tech adversaries as interrelated processes, this article bridges insights from intelligence studies, cyber security, and IR theory that have largely remained siloed. Empirically, it

extends the literature by demonstrating how these dynamics operated simultaneously across tactical, operational, and strategic levels in the Israeli intelligence failure of 7 October 2023, illustrating that surprise emerged not despite data abundance but because of it. In doing so, the article shifts the debate from whether technology can fail to how digital architectures themselves structure misperception, organizational rigidity, and adversarial opportunity, thereby offering a generalizable framework for analyzing strategic surprise in digitally advanced states.

The preceding analysis suggests that digitalization does not merely enhance state capacity. Rather, it fundamentally reshapes the environment in which intelligence, perception, and strategic decision-making occur. To understand strategic surprise in the twenty-first century, IR scholarship must account for the emergent properties of digital infrastructures and their interaction with organizational psychology, political culture, and adversarial strategy.

This section situates the concept of techno-digital vulnerability within broader debates in international relations, draws out the theoretical implications, and outlines how this framework extends or challenges existing approaches.

7.1. Rethinking Traditional Approaches to Strategic Surprise

The classical literature on surprise, such as work by Betts, Jervis, Bar-Joseph, and others, offers powerful analytic tools for understanding why states are blindsided by threats. These scholars emphasize cognitive bias, organizational dysfunction, interagency coordination failures, and political pressure. Despite the range of perspectives, a common theme unites them: intelligence failures arise because information is misinterpreted, ignored, or suppressed, and not because it is unavailable. The digital age adds a new layer of complexity. Digital systems generate vast quantities of information but also structure the way information is collected, processed, and interpreted. Traditional models of surprise did not anticipate environments in which automated sensors dominate collection, AI models shape expectations and offer predictions, and analysts rely on real-time dashboards, while leaders are inundated with data streams. Thus, while classical literature remains indispensable, it must be updated to account for how digital infrastructures create both new forms of blindness and new pathways for surprise. Techno-digital vulnerability suggests that surprise may increasingly occur not despite data abundance, but because of it. Data structures can mislead. Algorithms solidify assumptions rather than challenge them. The belief in digital omniscience narrows the range of plausible threat scenarios, making certain kinds of surprise more likely.

7.2. Technology, Power, and the Paradox of Capability

A central implication of the framework is that technological capability is not linear in its effects. Realist theory traditionally treats capability as additive: more power produces more security. Digital superiority appears to confirm this logic. Yet as Slayton (2017) and others have shown in the cyber domain, advanced systems generate new forms of fragility. For example, digital platforms often require tight coupling: interdependent components that operate in synchronization. Tight coupling is efficient, but it is also brittle. A small failure can cascade through the system. This insight resonates with Perrow's (1984) classic theory of complex systems accidents, where the very features that enhance system performance also increase the likelihood of catastrophic failure. Applied to IR, techno-digital vulnerability suggests that digital superiority may create returns to fragility. The more a state invests in digital tools to enhance surveillance, targeting, and intelligence, the more it becomes dependent on the integrity of those tools. And because adversaries can often disrupt or evade digital systems with low-cost methods, the technological advantage becomes a

form of structural exposure. This dynamic complicates traditional realist assumptions. It suggests that technological capability is not simply a multiplier of coercive power; it is also a generator of risk.

7.3. Liberal Openness, Transparency, and Strategic Exposure

Liberal IR theory emphasizes the benefits of openness: transparency reduces uncertainty, facilitates cooperation, and supports democratic accountability. In the digital era, openness is often celebrated as a normative good and a strategic advantage. Yet as Farrell and Newman (2019) note, interdependence also creates opportunities for exploitation.

Hypervisibility, that is, structural exposure of digitally open societies, poses a challenge to liberal assumptions. Public protest movements, online discourse, civilian mapping, digital service platforms, and ubiquitous mobile data can provide adversaries with a detailed picture of a state's internal vulnerabilities. This occurs even when the digital openness was not designed for external consumption.

Thus, techno-digital vulnerability introduces a new tension within liberal internationalism: the very openness that supports liberal governance may undermine national security. This is not an argument against digital democracy but a call to incorporate digital exposure into assessments of strategic risk. Democracies must find ways to preserve openness while mitigating the structural visibility it creates.

7.4. Constructivism, Identity, and Techno-Nationalist Hubris

Constructivist IR scholarship highlights how identities, narratives, and social meaning shape state behavior. Techno-digital vulnerability interacts deeply with these dynamics. Narratives of technological superiority that are common across advanced democracies and emerging powers alike shape organizational expectations and strategic assessments. States whose identity is bound up with technological innovation often view digital tools not merely as instruments but as sources of national pride and moral authority. This identity dimension matters because organizational cultures interpret technology through the lens of national self-conception. Techno-nationalist hubris can thus produce an overestimation of one's own digital capabilities and an underestimation of adversaries who adopt low-tech, analog, or hybrid strategies.

Constructivist theory, integrated with the techno-digital framework, suggests that strategic surprise is not merely a failure of information or cognition; it may also be a failure of identity, where narratives about digital superiority blind states to alternative possibilities.

7.5. Toward a Digital Theory of Surprise

Taken together, these insights point toward the need for an updated theory of strategic surprise. One that integrates digital infrastructures, sociotechnical systems, and cultural narratives into the core of analysis. Such a theory would recognize that digital systems reshape perception and structure intelligence routines. It also suggested that digital openness restructures vulnerability, and finally, that digital identities shape threat imagination. This theory does not replace classical approaches to surprise but extends them. Where earlier work emphasized the human element such as cognition, politics, and organizational dynamics, a digital theory of surprise adds a structural dimension: the role of the technological environment itself.

8. Implications for Policy and Practice

While this article is primarily conceptual, the framework has practical implications for digitally advanced democracies. If digital superiority creates forms of vulnerability, states must develop strategies to mitigate these risks without abandoning the benefits of technological innovation.

8.1. Rebalancing Intelligence Collection

Digital systems have tilted intelligence collection heavily toward SIGINT and other sensor-based modalities. This raises an intriguing question: whether the October 7 surprise would have still occurred had Israel possessed less sophisticated surveillance and intelligence technologies. How much less sophisticated would those capabilities have needed to be to avoid being blindsided by Hamas?

With the proven benefits of these technologies, the solution should come from another direction. The techno-digital vulnerability framework suggests that HUMINT, ethnographic insight, and contextual interpretation must be reemphasized. Human-based warning methods are often better equipped to detect analog or deceptive adversarial strategies that digital systems miss. From early reports, it seems that the IDI has already adopted this lesson. A senior IDI officer recently stated the following: "in the past there may have been a sense that technology could replace some of the people working with language, Iron Swords [the name Israel gave to the 2023–2025 war] demonstrated that in the end there is no substitute for the human for the ear, for the person who reads and knows how to interpret various expressions. This is our directive for the coming years: recruiting and empowering language specialists" (Ganot 2025).

8.2. Building Resilience Through Redundancy

Digital dependency makes intelligence organizations brittle. States should invest in analog redundancies, diversified data architectures, and decentralized analytic processes. Redundancy is often viewed as inefficient, but in a world where digital infrastructures can fail suddenly, redundancy is a source of resilience. This includes designing systems that can continue to function in degraded modes, training analysts to operate without real-time digital data, and ensuring that critical warning channels can survive attacks on digital nodes.

8.3. Treating Digital Openness as a Strategic Exposure

Democracies must acknowledge that their informational openness is a strategic vulnerability. Policymakers should encourage digital literacy not only to counter disinformation but to raise awareness of how public data can be exploited by adversaries. This may require public guidance on geolocation restrictions, political–military communication discipline, and the visibility of critical infrastructure. Unlike authoritarian states, democracies cannot close their digital ecosystems, but they can cultivate public practices that reduce unnecessary exposure.

8.4. Institutionalizing Dissent, Alternative Analysis, and Doctrinal Change

Digital illusion and techno-nationalist hubris suppress dissent. Intelligence organizations should institutionalize red-teaming exercises that explicitly challenge dominant digital assumptions. Analysts should be encouraged to consider how adversaries might exploit digital systems, avoid digital detection, or innovate using low-tech methods. The goal is to create organizational cultures that treat digital data as one source among many but not as the final arbiter of truth. Similarly, military and intelligence doctrine must reflect the reality that digital superiority is not synonymous with control. States should assume that adversaries will seek to degrade digital infrastructures, deceive automated systems, and exploit digital transparency. Doctrine must be updated accordingly. The possibility of fighting in environments where digital systems fail should no longer be treated as extraordinary; it should be assumed.

9. Conclusions

Digital superiority is one of the defining features of contemporary statecraft. States increasingly depend on sensors, data systems, and AI-driven analysis to make sense of complex strategic environments and to take action, including kinetic operations. The promise of digital power is irresistible: more data, better visibility, faster response, greater control. Yet as this article has argued, digital superiority also carries profound vulnerabilities. Techno-digital vulnerability offers a conceptual framework for understanding these risks. It shows how digital infrastructures generate illusions of informational completeness, create organizational dependencies that erode resilience, expose democratic societies to adversarial exploitation, and shape cultural narratives that distort threat assessment. These dynamics help explain why digitally advanced states remain vulnerable to strategic surprise in the twenty-first century. The Israeli experience of 7 October 2023 is only one illustration of this broader phenomenon, but it is a revealing one. It shows how digital power can become a source of strategic blindness. It underscores the need for intelligence organizations to cultivate interpretive humility, institutional diversity, and operational resilience.

More broadly, this article argues that IR scholarship must integrate digital systems into the study of strategic surprise. Traditional approaches remain essential, but they must be complemented by attention to how technology structures perception, organization, and vulnerability. Without such integration, the field risks misunderstanding the nature of threat and security in the digital age.

As states continue to invest in digital architectures, incorporate AI into intelligence workflows, and expand cyber capabilities, they will confront not only new opportunities but new dangers. The central task for scholars and practitioners is to understand and mitigate the vulnerabilities that arise not from technological inferiority but from digital superiority itself.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the author.

Conflicts of Interest: The author declares no conflicts of interest.

References

Allen, Gregory C. 2017. *Putin and Musk Are Right: Whoever Masters AI Will Run the World*. Washington, DC: Center for a New American Security. Available online: https://www.cnas.org/publications/commentary/putin-and-musk-are-right-whoever-masters-ai-will-run-the-world (accessed on 1 September 2025).

Amidror, Jacob. 2002. *Thoughts About Military and Security*. Tel-Aviv: Itzuv.

Arnon, Ruth, Michael Sela, and Colin Shindler. 2016. *Ephraim Katchalski-Katzir*. London: Royal Society. Available online: https://royalsocietypublishing.org/doi/pdf/10.1098/rsbm.2016.0015 (accessed on 1 January 2026).

Ashkenazi, Avi. 2025. The Treasure Hamas Stole from Israel: The IDF's Dramatic Decision for the Fighters. *Maariv*. Available online: https://www.maariv.co.il/news/military/article-1177500 (accessed on 1 January 2026).

Azulai, Yuval. 2025. Israeli Defense Exports at New High of 15 Billion USD. *Calcalist*. Available online: https://www.calcalist.co.il/local_news/article/sks9x5pzee (accessed on 17 September 2025).

Bar-Joseph, Uri, and Rose McDermott. 2017. *Intelligence Success and Failure: The Human Factor*. Oxford: Oxford University Press.

Ben Gurion, David. 1949. A Vision and a Path. 1958. In *Ben Gurion's Thought*. Edited by Yaacov Becker. Tel-Aviv: Yavne.

Betts, Richard K. 1978. Analysis, War, and Decision: Why Intelligence Failures Are Inevitable. *World Politics* 31: 61–89. [CrossRef]

Betts, Richard K. 2007. *Enemies of Intelligence: Knowledge and Power in American National Security*. New York: Columbia University Press.

Bob, Yonah J. 2025. New IDF Probe Reveals Failures in Five October 7 Investigations, Which Need to be Redone. *Jerusalem Post*. Available online: https://www.jpost.com/israel-news/politics-and-diplomacy/article-873402 (accessed on 11 November 2025).

Breznitz, Dan. 2007. *Innovation and the State: Political Choice and Strategies for Growth in Israel, Taiwan, and Ireland*. New Haven: Yale University Press.

Bryant, Steven L. 2011. The Dangers of an Over-Reliance on Technology. Master's thesis, Joint Forces Staff College, Norfolk, VA, USA. Available online: https://apps.dtic.mil/sti/tr/pdf/ADA545545.pdf (accessed on 1 January 2026).

Cohen, Erez. 2011. The Development of the High tech industry in Israel, and government policy to Support it. In *Connected: Politics, Technology and Society in Israel*. Edited by Erez Cohen and Azi Lev-on. Tel-Aviv: Israeli Association of Political Science.

Eiran, Eiran, Ofer Guterman, and David Siman-Tov. 2025. The vanishing watchman: The rise and decline of early warning. *Intelligence and National Security* 40: 863–85. [CrossRef]

Eppler, Martin J., and Jeanne Mengis. 2004. The Concept of Information Overload: A Review of Literature from Organization Science, Accounting, Marketing, MIS, and Related Disciplines. *The Information Society* 20: 325–44. [CrossRef]

Eyal, Nadav. 2024. The Bomb and the Failure. *YNET*. Available online: https://www.ynet.co.il/yedioth/article/yokra14111106 (accessed on 12 November 2025).

Eyal, Nadav. 2025. Primarily Published: Security Establishment Admits That Shin Bet, Unit 504 and Mossad Did Not Hold Any Significant Agent Within Hamas Leadership for Some 20 Years. *YNET*. Available online: https://www.ynet.co.il/news/article/s1zuk1oqwe (accessed on 11 November 2025).

Farrell, Henry, and Abraham Newman. 2019. Weaponized Interdependence: How Global Economic Networks Shape State Coercion. *International Security* 44: 42–79. [CrossRef]

Finkel, Meir. 2006. The Cult of Technology in the IDF: The IDF's Cult of Technology: Restoring Balance to Ground Force Development. *Maarchot* 407: 40–45.

Flamer, Netanel. 2024. *The Hamas Intelligence War Against Israel*. Cambridge: Cambridge University Press.

Freilich, Charles. 2018. *Israeli National Security: A New Strategy for an Era of Change*. Ithaca: Cornell University Press.

Ganot, Gal. 2025. In Military Intelligence, They Are Studying the Yemeni Dialect: There Is No Substitute for the Human Ear. The Lesson from 7/1: An Exclusive Look. *YNET*. Available online: https://www.ynet.co.il/news/article/yokra14431208 (accessed on 2 January 2026).

Gartzke, Erik. 2013. The Myth of Cyberwar. *International Security* 38: 41–73. [CrossRef]

Halabi, Einav. 2023. They Destroyed the Fighters' 'Eyes,' Blew Up the Fence and Raided: The Footage from the Surprise Attack, and the Missed Warning Signs. *YNET*. Available online: https://www.ynet.co.il/news/article/byj4jpcl6 (accessed on 23 September 2025).

Halevi, Herzi. 2017. Director of IDI Opening Comments. *Modi'in Halacha U'Ma'ase* 2: 1.

Harris, Leon. 2025. Your Taxes: Israel's R&D Edge Over Other OECD Countries. *Jerusalem Post*. Available online: https://www.jpost.com/business-and-innovation/article-868577 (accessed on 2 January 2026).

Herzel, Theodor. 1902. *Old New Country*. Warsaw: Zionist Organization.

Heuer, R. 1999. *Psychology of Intelligence Analysis*. Washington, DC: CIA Press.

Heuer, Richards J., and Randolph H. Pherson. 2015. *Structured Analytic Techniques for Intelligence Analysis*, 2nd ed. Washington, DC: CQ Press.

Israel Defense Force (IDF). 2021. Construction of the Barrier Around the Gaza Strip Has Been Completed. This Is What It Looks Like. *IDF Internet Site*. Available online: https://www.idf.il/%D7%90%D7%AA%D7%A8%D7%99-%D7%99%D7%97%D7%99%D7%93%D7%95%D7%AA/%D7%A4%D7%99%D7%A7%D7%95%D7%93-%D7%94%D7%93%D7%A8%D7%95%D7%9D/%D7%9B%D7%9C-%D7%94%D7%9B%D7%AA%D7%91%D7%95%D7%AA/2021/%D7%9E%D7%9B%D7%A9%D7%95%D7%9C-%D7%A8%D7%A6%D7%95%D7%A2%D7%AA-%D7%A2%D7%96%D7%94-%D7%97% D7%95%D7%9E%D7%94-%D7%94%D7%A1%D7%AA%D7%99%D7%99%D7%9E%D7%94-%D7%91%D7%A0%D7%99%D7%99%D7%94/ (accessed on 2 January 2026).

Israel Defense Intelligence (IDI). 2021. The Innovative 'Gazit' Institute Was Inaugurated Within the Research Department. Available online: https://www.idf.il/%D7%90%D7%AA%D7%A8%D7%99-%D7%99%D7%97%D7%99%D7%93%D7%95%D7%AA/%D7%90%D7%92%D7%A3-%D7%94%D7%9E%D7%95%D7%93%D7%99%D7%A2%D7%99%D7%9F/%D7%9B%D7%9C-%D7%94%D7%9B%D7%AA%D7%91%D7%95%D7%AA/2021/%D7%9E%D7%9B%D7%95%D7%9F-%D7%92%D7%96%D7%99%D7%AA-%D7%90%D7%9E%D7%9F-%D7%90%D7%92%D7%A3-%D7%94%D7%9E%D7%95%D7%93%D7%99%D7%A2%D7%99%D7%9F-%D7%97%D7%98%D7%99%D7%91%D7%AA-%D7%94%D7%9E%D7%97%D7%A7%D7%A8/ (accessed on 2 January 2026).

Israel Trade Mission in Keniya. 2022. Israel Border Security Technology: Smart Walls and All. Available online: https://itrade.gov.il/kenya/israel-border-security-technology-smart-walls-and-all/ (accessed on 1 January 2026).

Jervis, Robert. 2010. *Why Intelligence Fails: Lessons from the Iranian Revolution and the Iraq War*. Ithaca: Cornell University Press.

Katz, Brian. 2020. The Collection Edge: Harnessing Emerging Technologies for Intelligence Collection. *CSIS Brief*. Available online: https://www.csis.org/analysis/collection-edge-harnessing-emerging-technologies-intelligence-collection (accessed on 2 January 2026).

Katzir, Aron. 1971. *The Crucible of the Scientific Revolution*. Tel-Aviv: Am Oved.

Keohane, Robert, and Joseph Nye. 2012. *Power and Interdependence*, 4th ed. Boston: Longman.

Limor, Yoav. 2021. Deputy Commander of 8200: There is No Place That Can Be Hacked. *Israel Hayom*. Available online: https://www.israelhayom.co.il/magazine/hashavua/article/4563280 (accessed on 3 January 2026).
Lindsay, Jon. 2013. Stuxnet and the Limits of Cyber Warfare. *Security Studies* 22: 365–404. [CrossRef]
Maariv Staff. 2022. The Munitions in Truck No. 8: Kochavi Confirmed that the IDF Struck a Convoy on the Syria-Iraq Border. *Maariv Online*. Available online: https://www.maariv.co.il/news/military/article-965266 (accessed on 6 November 2025).
Maimon, Moshe, and Udi Alony. 2019. The Economic Issue is Burning in Our Bones. *Funder*. Available online: https://www.funder.co.il/article/96733 (accessed on 4 November 2025).
Mearsheimer, John. 2001. *The Tragedy of Great Power Politics*. New York: Norton.
Morgenthau, Hans. 1967. *Politics Among Nations: The Struggle for Power and Peace*, 4th ed. New York: Alfred A. Knopf. First published in 1948.
Ortal, Eran. 2021. The Fly on the Elephant's Back: The Campaign between Wars in Israel's Security Doctrine, INSS. Available online: https://www.inss.org.il/strategic_assessment/the-fly-on-the-elephants-back-the-campaign-between-wars-in-israels-security-doctrinee/ (accessed on 3 January 2026).
Parasuraman, Raja, and Dietrich M. Manzey. 2010. Complacency and Bias in Human Use of Automation: An Attentional Integration. *Human Factors: The Journal of the Human Factors and Ergonomics Society* 52: 381–410. [CrossRef] [PubMed]
Penslar, Derek. 1991. *Zionism and Technocracy: The Engineering of Jewish Settlement in Palestine, 1870–1918*. Bloomington: Indiana University Press.
Peña, Carlos. 2024. 'It's Easy to Get Lost: The Temptation of Overreliance on Technology'. *Warroom*. December 5. Available online: https://warroom.armywarcollege.edu/articles/temptation-of-technology/ (accessed on 3 January 2026).
Perrow, Chrles. 1984. *Normal Accidents: Living with High-Risk Technologies*. New York: Basic Books.
Plant CA. 2023. Blind Spots: Our Over-Reliance on Technology Creates more Obstacles than Necessary. *Plant*, August 14. Available online: https://www.plant.ca/features/blind-spots-our-over-reliance-on-technology-creates-more-obstacles-then-necessary (accessed on 8 November 2025).
Posen, Barry. 2003. Command of the Commons. *International Security* 28: 5–46. [CrossRef]
Reinharz, Jehuda, and Motti Golani. 2024. *Chaim Weizmann: A Biography*. Waltham: Brandeis University Press.
Schif, E. 2024. The Shrapnel in the Backside Doctrine. *YNET*. Available online: https://www.ynet.co.il/yedioth/article/yokra14008275 (accessed on 2 January 2026).
Senor, Dan, and Saul Singer. 2009. *Start-Up Nation: The Story of Israel's Economic Miracle*. New York: Council of Foreign Relations.
Serena, Chad C., and Colin P. Clarke. 2019. America's National Defense Strategy and the Paradox of Technology. *RAND Corporation Commentary*. Available online: https://www.rand.org/pubs/commentary/2019/02/americas-national-defense-strategy-and-the-paradox.html (accessed on 3 November 2025).
Shchwab, Klaus. 2016. *The Fourth Industrial Revolution*. New York: Crown Business.
Siman-Tov, David, and Ofer Guterman, eds. 2025. *Intelligence the Seventh of October*. Tel-Aviv: Maarachot.
Slayton, Rebecca. 2017. *Arguments That Count: Physics, Computing, and Missile Defense, 1949–2012*. Cambridge: MIT Press.
Technion UK. 2024a. AI Tool Predicts Rocket Fire on Israel, Finds Best Time to Shower. Available online: https://technionuk.org/news-post/ai-tool-predicts-rocket-fire-on-israel-finds-best-time-to-shower/ (accessed on 2 January 2026).
Technion UK. 2024b. Israel's Technion Ranked #1 Worldwide in Digital Education. Available online: https://technionuk.org/news-post/israels-technion-ranked-1-worldwide-in-digital-education/ (accessed on 2 January 2026).
U.S. Government Accountability Office GAO. 2018. *DOD Just Beginning to Grapple with Scale of Vulnerabilities*; Washington, DC: GAO. Available online: https://www.gao.gov/assets/gao-19-128.pdf (accessed on 2 January 2026).
Williams, D. 2001. Is the West's reliance on technology the panacea for future conflict or its Achilles' heel? *Defence Studies* 1: 38–56. [CrossRef]
Winkler, Stephanie Christine. 2025. New and Old Cold Wars: The Tech War and the Role of Technology in Great Power Politics. *Global Studies Quarterly* 5: ksaf038. [CrossRef]
Zegart, Amy. 2022. *Spies, Lies, and Algorithms: The History and Future of American Intelligence*. Princeton: Princeton University Press.
Zeitun, Yoav. 2025. 1175 Terrorists in the First Wave, Against 671 Soldiers: 'Don't be Surprised if They Reach Tel Aviv' | The Dramatic Orders in the Command Bunker, Minute by Minute. *YNET*. Available online: https://www.ynet.co.il/news/article/by6miz091x (accessed on 22 December 2025).

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.