

Strategic Stability in an Era of Hybrid Warfare: The Case of Iran and Israel

Bilkisu Usman Bala

Department of International Relations, Skyline University Nigeria

balabilkisuusman@gmail.com

Yemi Daniel Ogundare PhD

Department of International Relations, Skyline University Nigeria

ogundareyemi20@gmail.com

Nyam Elisha Yakubu PhD

Department of International Relations, Skyline University Nigeria

nyamelishayakubu@gmail.com

Abstract

The Iran-Israel rivalry has emerged as one of the most consequential cases for understanding strategic stability under conditions of hybrid warfare. Strategic stability serves as the primary theoretical framework used in this study, which employs a qualitative case study approach based on the systematic analysis of secondary sources, including policy documents, official statements, scholarly literature, and security reports, to examine contemporary shifts in the Middle Eastern security landscape. Traditional deterrence theory, developed primarily in the nuclear age, assumed identifiable actors, clear thresholds, and relatively predictable escalation pathways. The Iran–Israel confrontation challenges these assumptions. It is characterized by persistent competition below the threshold of full-scale war, combining cyber operations, proxy warfare, precision strikes, information campaigns, economic coercion, maritime disruption, and increasingly direct missile and drone exchanges. The findings of this article argue that hybrid warfare has transformed strategic stability from a condition of mutual restraint into a dynamic process of continuous risk management. While hybrid methods can delay conventional war by providing flexible options for calibrated coercion, they also increase the risks of misperception, inadvertent escalation, and crisis instability. The Iran-Israel case demonstrates that strategic stability in the twenty-first century depends less on preventing conflict altogether than on managing escalation across interconnected military and non-military domains.

Keywords: Deterrence, Strategic Stability, Hybrid Warfare, Multi-Domain Deterrence, Iran-Israel rivalry

1.0 Introduction

Strategic stability has traditionally referred to a condition in which adversaries lack incentives to initiate major conflict, especially nuclear war. Classical formulations focused on survivable second-strike capabilities, rational decision-making, and stable deterrence relationships. Yet contemporary conflicts increasingly unfold in the ambiguous space between peace and war (Kroenig, 2024). Hybrid warfare, defined as the integrated use of conventional, irregular, cyber, informational, economic, and proxy tools, has become a dominant mode of interstate competition (Kühn, 2023).

Among contemporary rivalries, the Iran–Israel case offers a particularly valuable framework for examining the relationship between hybrid warfare and strategic stability because it combines sustained proxy competition, technological innovation, ideological confrontation, and periodic direct military exchanges without escalating into full-scale conventional war. Unlike cases such as Russia-Ukraine, which evolved into large-scale interstate warfare, or China-Taiwan, where direct military confrontation remains largely prospective, the Iran-Israel rivalry illustrates how states manage prolonged confrontation across multiple interconnected domains while attempting to avoid uncontrolled escalation.

For decades, both states engaged in indirect confrontation through proxies, covert action, cyber sabotage, and limited strikes (Adan, 2026). However, recent developments, especially since 2024-2026, have revealed a transition from shadow war to overt, though still limited, interstate confrontation. This evolution raises fundamental questions: Can strategic stability survive under conditions of persistent hybrid conflict? How do new technologies and multi-domain operations affect deterrence? And what lessons does the Iran–Israel case offer for broader international security?

This article contends that hybrid warfare has not eliminated deterrence; rather, it has reconfigured it. Strategic stability now rests on adaptive escalation control, resilience, and the capacity to signal resolve without triggering uncontrolled war.

2.0 Theoretical Framework: Rethinking Strategic Stability

For much of the twentieth century, strategic stability was understood in relatively straightforward terms. It described a condition in which rival states, particularly major military powers, had little incentive to initiate war because the likely costs would far outweigh any potential benefits (Suh, 2023). At its core, strategic stability was about maintaining a balance so durable and predictable that neither side would see advantage in upsetting it. This classical understanding rested on three interconnected pillars: crisis stability, arms race stability, and deterrence stability (Bolt, 2025).

Crisis stability refers to a situation in which, during moments of heightened tension, neither side feels compelled to strike first (Fink, 2017). The logic is simple but profound: if both actors believe that waiting does not place them at a decisive disadvantage, the pressure for preemptive action is reduced (Zhao, 2024). In such an environment, leaders have the time and space to assess developments, communicate intentions, and pursue de-escalatory options. The absence of a “use it or lose it” mentality is therefore central to maintaining peace during crises.

Arms race stability, by contrast, concerns the long-term military competition between rivals. Stability exists when neither state believes that rapidly expanding its military capabilities will provide a decisive strategic edge (Peczeli, 2023). If both sides recognize that attempts to outbuild one another are unlikely to produce meaningful superiority, the incentive for costly and destabilizing arms races diminishes (Na'inna & Anti-Dwanso, 2022). This helps preserve equilibrium by discouraging spirals of military competition that can heighten insecurity and mistrust.

Deterrence stability completes the triad. It exists when both sides are convinced that the costs of aggression will outweigh any conceivable gains (Michael, 2021). In essence, deterrence works when the prospect of retaliation or the broader consequence of conflict is sufficiently severe to dissuade either party from initiating hostilities (Patrick, 2012). Stability, in this sense, depends not on trust or goodwill, but on a shared understanding of the unacceptable price of war.

However, the rise of hybrid warfare has profoundly complicated this traditional framework. Contemporary conflict no longer unfolds solely through conventional military means. Instead, states increasingly employ a blend of cyber operations, proxy warfare, disinformation campaigns, economic coercion, covert action, and limited kinetic strikes (Weissmann, 2021). These tools blur the line between war and peace, making strategic interactions far less predictable. Scholars such as Mazarr (2021), as well as Ucko and Marks (2020), have argued that contemporary strategic competition increasingly operates within this “gray zone” between peace and open warfare, where states pursue coercive objectives while deliberately avoiding escalation into full-scale conflict. Their work is particularly important because it helps bridge the gap between classical deterrence theory and the realities of hybrid warfare by demonstrating how deterrence must now function across multiple interconnected domains simultaneously.

One of the defining features of hybrid warfare is ambiguity. Actions are often deliberately designed to obscure their source, purpose, or intended effect (Li & Liu, 2021). Cyberattacks, for instance, may be difficult to attribute with certainty, while covert operations may be conducted under layers of deniability (Mumford & Carlucci, 2022). This uncertainty complicates decision-making, as leaders may struggle to determine who is responsible, what message is being sent, or whether an isolated incident is part of a broader campaign.

Asymmetry further reshapes the strategic landscape. Hybrid warfare allows weaker actors to challenge stronger adversaries through unconventional means. Rather than competing symmetrically in conventional military power, states can exploit vulnerabilities in cyberspace, leverage proxy forces, or engage in information warfare (Mitrovic, 2017). This expands the range of available tools and enables actors with fewer traditional resources to impose significant costs on more powerful opponents.

Incrementalism is another important characteristic. Hybrid strategies often rely on a series of small, calibrated actions that remain below the threshold likely to trigger full-scale war. These “gray zone” operations allow states to pursue strategic objectives gradually, testing boundaries and probing red lines without crossing them outright (Ucko & Marks, 2020). Yet while each individual action may seem limited, their cumulative effect can steadily alter the strategic balance.

Perhaps most importantly, hybrid warfare introduces a high degree of cross-domain interaction. Actions in one domain can have cascading consequences in others. A cyberattack on critical infrastructure, for example, may provoke a military response (North Atlantic Treaty Organization, 2024). Maritime incidents may trigger diplomatic crises. Information operations can shape public perceptions and influence political decision-making, which in turn affects military calculations. The interconnectedness of these domains means that escalation is no longer confined to a single arena (Victoria, 2024).

Consequently, strategic stability can no longer be understood as a fixed or permanent condition. It is no longer a stable equilibrium that, once achieved, simply endures. Instead, it has become a dynamic and continually evolving process (Bolt, 2025). Stability today depends on constant signaling, careful calibration, and the ability of adversaries to manage risks across multiple domains simultaneously.

In this new environment, strategic stability is less about eliminating conflict altogether and more about preventing competition from spiraling into uncontrolled war. It is contingent rather than absolute, fluid rather than static, and continuously renegotiated through the actions, perceptions, and responses of the actors involved (Iroye et al., 2026). The challenge for contemporary strategists is therefore not merely to preserve stability, but to adapt its meaning to an era in which the boundaries between peace and conflict have become increasingly blurred.

2.1 Methodology

This study adopts a qualitative, interpretivist approach to examine how hybrid warfare is reshaping strategic stability in the contemporary Middle East. Using the Iran-Israel rivalry as a conceptual case study, the article combines theoretical analysis with an empirical examination of geopolitical developments between 2024 and 2026. The case was selected because it offers a particularly relevant example of sustained interstate competition conducted across multiple domains including cyber operations, proxy warfare, covert action, information campaigns, precision strikes, and calibrated missile exchanges without escalating into prolonged full-scale conventional war. Unlike Russia–Ukraine, which evolved into open interstate warfare, or China-Taiwan, where conflict remains largely prospective, the Iran-Israel rivalry demonstrates how adversaries manage persistent confrontation while attempting to maintain escalation control (Popalzay et al., 2025). The study relies on qualitative analysis of secondary sources, including scholarly literature, policy reports, official government statements, military communiqués, speeches, and strategic assessments. Through discursive and thematic analysis, the article identifies recurring patterns in deterrence signaling, escalation management, and hybrid conflict dynamics. Rather than testing a single causal hypothesis, the study seeks to contribute conceptually to contemporary debates by reinterpreting strategic stability as a dynamic and continuously negotiated process shaped by hybrid warfare, technological transformation, and multi-domain interstate competition.

2.2 Genesis of the Iran-Israel Rivalry

Phase I: Indirect and Proxy Competition (Late 1970s-2010s)

For much of the past four decades, the rivalry between Iran and Israel was defined not by open warfare, but by indirect confrontation (Zamin & Nasir, 2026). Following the 1979 Islamic Revolution, both states viewed each other as major strategic adversaries, yet they generally avoided direct military engagement (Pivariu, 2026). Instead, their competition unfolded through proxies, covert operations, intelligence activities, and carefully calibrated regional maneuvering a strategy that allowed each side to pursue its interests while minimizing the risk of full-scale war.

For Iran, this strategy was rooted in "forward defense." Rather than waiting for threats to reach its own borders, Tehran sought to project influence outward by cultivating alliances with non-state actors and sympathetic regional movements (Aladhami & Abbas, 2025). Groups such as Hezbollah, particularly following its formation in the early 1980s, became central to this approach. Through these partnerships, Iran extended its strategic reach across the Middle East, creating layers of deterrence and influence that could be activated when necessary (Badawi, 2026). This network not only enhanced Iran's regional presence but also served as a means of countering Israeli and Western pressure.

Israel responded with a different but equally calculated strategy, often referred to as the "campaign between wars." While this doctrine was informal for years, Israel's deep military involvement in the Syrian Civil War starting around 2013 solidified it as a core operational framework. This doctrine focused on preventing Iran from entrenching itself militarily near Israeli borders and from transferring advanced weaponry to its allies, particularly Hezbollah (Wyss, 2024). Israeli operations frequently targeted Iranian military installations, arms shipments, and logistical networks, especially in Syria. These strikes were designed to degrade Iran's capabilities, disrupt its regional ambitions, and maintain Israel's strategic advantage, all without triggering a broader war (Khatib, 2026).

This prolonged period of indirect competition created a paradoxical form of stability. Hostility was constant, and the risk of escalation was ever present, yet both sides appeared to recognize the dangers of direct confrontation. Their actions were often aggressive, but they were also carefully measured. Each sought to impose costs on the other while remaining below the threshold that would likely provoke an all-out conflict. In this sense, the rivalry was highly adversarial but also bounded by mutual caution. Proxy warfare, covert action, and limited strikes became tools for managing competition rather than unleashing unrestricted war. The result was a tense but relatively stable strategic equilibrium—one in which conflict was real, persistent, and often violent, yet constrained by an implicit understanding of the catastrophic consequences that direct war could bring.

Phase II: The Hybrid Shadow War (2010s - 2024)

Over time, the rivalry evolved beyond mere proxy competition into what can best be described as a hybrid shadow war (Politics Society, 2026). While direct military confrontation was still largely avoided, the contest became far more sophisticated, multidimensional, and covert. The pivot into

this phase is most clearly marked by the dawn of the Stuxnet cyberattack discovered in 2010, alongside an intensified campaign of targeted assassinations within Iran. These events expanded the battlefield beyond traditional military arenas to include cyberspace, maritime routes, intelligence networks, and information domains (German et al., 2026; Sciarrone, 2017).

In this phase, both states increasingly relied on a blend of unconventional tools to weaken one another without crossing the threshold into open war. Cyber operations became a particularly important instrument. Attacks on critical infrastructure, communication systems, and sensitive networks allowed each side to disrupt the other's capabilities while preserving a degree of deniability (Azeroual et al., 2026; George et al., 2024). In cyberspace, attribution is often uncertain, making it an ideal arena for strategic competition below the level of conventional conflict.

The maritime domain also emerged as a key theater of rivalry, notably intensifying into a "tit-for-tat" tanker war between 2019 and 2021. Commercial vessels, oil tankers, and other strategic shipping assets in the Persian Gulf and the Red Sea became targets of disruption and harassment (Kotait & Ismail, 2025). These incidents were not merely symbolic; they carried significant economic and strategic implications, affecting trade routes, energy flows, and regional security calculations.

Covert operations formed another central pillar of this shadow conflict. Targeted assassinations of military commanders, intelligence operatives, and nuclear scientists became a means of degrading strategic capabilities while sending powerful deterrent signals (Bluth, 2025; Karahalios, 2026). Likewise, sabotage operations against sensitive facilities—particularly those linked to military or nuclear development were designed to delay progress, impose costs, and create uncertainty within the adversary's strategic planning.

Psychological and information operations also played an increasingly important role. Both sides sought not only to inflict material damage but also to shape perceptions, undermine confidence, and project strength (Hiruni, 2024; Shahbazi & Bunker, 2024). These efforts were aimed at influencing political leadership, military decision-making, and public opinion, both domestically and internationally.

What made this phase particularly distinctive was its reliance on plausible deniability. Each side could signal resolve and impose costs without formally claiming responsibility. This ambiguity provided strategic flexibility. It allowed both Iran and Israel to retaliate, deter, and compete aggressively while reducing the immediate risk of escalation into full-scale war (Mekelberg, 2026). In effect, the hybrid shadow war became a mechanism for managing rivalry under conditions of intense hostility. It enabled both states to test limits, demonstrate capability, and preserve deterrence, all while avoiding the catastrophic consequences of direct military confrontation (Khan, 2024). Conflict remained persistent and often highly consequential, but it was carefully calibrated to remain below the threshold of open war.

Phase III: Direct Limited Conflict (2024 - 2026)

The period between 2024 and 2026 marked a significant and unprecedented turning point in the long-standing rivalry (PW Live, 2026; Institute for Economics and Peace, 2026). For decades, both

states had managed their confrontation through the shadows. The definitive breaking point occurred in April 2024, when Iran launched a massive, direct missile and drone barrage against Israel in retaliation for a strike on its diplomatic compound in Damascus. This historic shift shattered the old playbook, moving the conflict into a highly overt and dangerous phase.

Iran increasingly moved away from an exclusive reliance on proxy forces and adopted a more direct approach to deterrence and retaliation (Heiran-Nia, 2026). Rather than acting solely through allied non-state actors, Tehran demonstrated a growing willingness to employ its own military capabilities, including ballistic missiles, drones, and coordinated regional operations directly from Iranian soil (Shankar, 2026). This shift reflected both confidence in its expanding arsenal and a desire to signal that it could respond directly when its interests or assets were threatened.

Israel, for its part, also adjusted its strategic posture. Traditionally focused on targeting Iranian proxies and regional infrastructure, Israel became more prepared to strike Iranian territory itself when it perceived critical threats (Manara Magazine, 2026). This represented a notable escalation in its operational doctrine. Direct attacks on Iranian soil carried far greater symbolic and strategic implications than earlier operations confined to third-party theaters such as Syria or Lebanon (Institute for Economics and Peace, 2026).

The result has been the emergence of a new phase of rivalry one characterized by direct but still limited military confrontation. Unlike full-scale war, these exchanges remain carefully calibrated. Both sides continue to exercise restraint, seeking to impose costs and demonstrate resolve without triggering an uncontrollable escalation (Yılmaz, 2026). Yet the threshold separating indirect competition from direct conflict has clearly been crossed.

Importantly, this new phase does not replace hybrid warfare; rather, it exists alongside it. Cyberattacks, covert operations, proxy activities, and information campaigns continue to play central roles. What has changed is that these tools are now complemented by occasional overt military exchanges (Azdejković et al., 2025). The rivalry has therefore become more complex, blending traditional deterrence with hybrid tactics and limited direct force.

This evolution has profound implications for regional security. The coexistence of direct military action and hybrid competition increases both the intensity and unpredictability of the conflict. While both Iran and Israel still appear intent on avoiding all-out war, the risks of miscalculation, rapid escalation, and unintended consequences have grown considerably. The Iran-Israel rivalry has entered a more volatile era a delicate and dangerous balance in which overt military exchanges occur within a broader framework of hybrid competition that is inherently less stable and far more difficult to manage (Khatun, 2026).

2.3 Hybrid Warfare and the Transformation of Deterrence

From Deterrence by Denial to Deterrence by Punishment

For many years, Iran based its security strategy on what scholars describe as deterrence by denial. The essence of this approach was to make aggression against Iran too difficult, costly, or uncertain to succeed. Rather than relying solely on direct military confrontation, Tehran sought to protect

itself by building strategic depth across the region (Maulana, 2024). This involved cultivating an extensive network of allied non-state actors, regional partners, and proxy forces capable of extending Iran's reach far beyond its borders. Through this network, Iran aimed to create multiple layers of defense. Any attack on Iranian interests could potentially trigger responses from allied groups operating in different theaters, thereby complicating an adversary's calculations (Roman, 2026; Iran International, 2026). This strategy provided both insulation and leverage, allowing Iran to project power indirectly while reducing its own vulnerability to direct military retaliation.

However, over time, the limitations of this model became increasingly apparent. Israel's persistent intelligence penetration, targeted operations, and repeated strikes against Iranian assets and proxy networks revealed vulnerabilities in Tehran's forward-defense architecture (Khatib, 2026). The effectiveness of some proxy forces also came under strain, whether because of operational setbacks, internal constraints, or the growing sophistication of Israeli countermeasures (Pokorny, 2026). As these pressures mounted, Iran's traditional reliance on deterrence by denial began to look less sufficient.

In response, Tehran has increasingly shifted toward a strategy of deterrence by punishment. Rather than merely seeking to prevent attacks by complicating an adversary's options, Iran now appears more willing to threaten and, when necessary, carry out direct retaliation (Heiran-Nia, 2026; Rawat, 2026). This profound doctrinal shift found its definitive empirical anchor in April 2024, when Tehran launched a massive, unprecedented salvo of over 300 ballistic missiles, cruise missiles, and armed drones directly from Iranian soil targeting Israel. This operation, triggered by a deadly Israeli strike on Iran's diplomatic compound in Damascus, shattered decades of proxy-reliance. By executing this strike, and a subsequent massive ballistic missile barrage later that year, Iran demonstrated a calculated willingness to bypass its traditional intermediaries and impose immediate, visible, and state-level costs on its adversaries (Young, 2026). This approach is designed not simply to absorb or deflect attacks, but to ensure that any aggression will be met with a painful and unmistakable direct response.

Israel, meanwhile, maintains a markedly different deterrence posture. Its strategy is built on a combination of preemption, superior intelligence capabilities, precision strike capacity, and highly advanced defensive systems (Pivariu, 2026). Israeli doctrine emphasizes the importance of identifying and neutralizing threats before they fully materialize. Its ability to gather intelligence, conduct surgical operations, and intercept incoming threats through layered missile defense gives it considerable strategic flexibility (Shapira, 2026). An additional dimension of Israel's deterrent posture lies in its longstanding policy of strategic ambiguity regarding its nuclear capabilities. By neither officially confirming nor denying its nuclear arsenal, Israel preserves uncertainty in the minds of potential adversaries (Young, 2026). This ambiguity itself serves as a powerful deterrent, reinforcing the perception that escalation beyond certain thresholds could carry catastrophic consequences.

The result is an inherently asymmetric deterrence relationship. Iran and Israel rely on different tools, different doctrines, and different pathways to influence each other's behavior. Iran increasingly emphasizes retaliation and cost imposition, while Israel combines prevention, technological superiority, and ambiguity (Azimi, 2026). Each side seeks to deter the other, but they do so through fundamentally different strategic logics. This asymmetry makes the relationship

both resilient and unstable. Resilient, because both sides possess credible means of imposing costs. Unstable, because their differing approaches can create misunderstandings, miscalculations, and unpredictable escalation dynamics. In this evolving environment, deterrence remains intact, but it is more complex, contested, and fragile than ever before.

In the contemporary strategic environment, deterrence between Iran and Israel no longer operates within a single military dimension. Instead, it has expanded into a multi-domain system in which power is exercised, signaled, and contested across several interconnected arenas at the same time (Haider, 2026; Heiran-Nia, 2026). This shift reflects the broader transformation of modern conflict, where the boundaries between war and peace, and between military and non-military instruments, have become increasingly blurred (Heiran-Nia, 2026).

Today, deterrence functions simultaneously across military, cyber, maritime, economic, informational, and diplomatic domains (Dolan, 2025; Keinonen, 2023). In the military sphere, both states rely on conventional and unconventional capabilities ranging from missile systems and airpower to proxy forces and special operations to signal resolve and impose costs (U.S. Army, 2025). In cyberspace, operations are used to disrupt infrastructure, gather intelligence, and demonstrate vulnerability without necessarily triggering immediate kinetic responses.

The maritime domain has also become increasingly important, particularly in strategically sensitive waterways such as the Persian Gulf and the Red Sea, where disruptions to shipping and energy flows can carry significant economic and political consequences (Donelli, 2025). At the same time, economic instruments such as sanctions, trade restrictions, and energy leverage play a central role in shaping strategic calculations and constraining adversary behavior.

Information and psychological operations further expand the scope of deterrence. Narratives, media messaging, and strategic communication are used to influence perceptions, shape domestic and international opinion, and project strength or vulnerability (Kaprisma, 2020). Diplomatic engagement, meanwhile, provides an additional layer through which states signal intentions, manage escalation, and seek external support or restraint from other international actors.

Cross-Domain Causal Linkages

Crucially, these domains do not function as isolated silos; rather, they interact dynamically, where non-kinetic operations directly shape and accelerate kinetic military decisions. This causal relationship is vividly illustrated by the integration of offensive cyber operations into conventional warfighting doctrines to pave the way for kinetic strikes. For instance, in modern escalatory sequences, a state may launch a highly targeted cyberattack 48 to 72 hours prior to an aerial operation, specifically designed to compromise the adversary's municipal utilities, regional command-and-control servers, or air-defense radar networks. By using digital tools to blind tracking capabilities and sow communication bottlenecks, strategic planners create an immediate window of physical vulnerability. This cyber-enabled disruption does not merely exist below the threshold of war; it serves as the direct catalyst for subsequent high-precision, kinetic military decisions, determining the exact timing and success of physical airstrikes. Conversely, the interaction also flows from kinetic actions back into the digital and informational domains. Physical strikes against critical command centers or state broadcasting facilities are frequently

paired with immediate cyber-hijacking of media feeds to wage psychological warfare, or answered by state-sponsored hacktivist groups deploying data-wiping malware in retaliation.

In this multi-domain environment, success or superiority in one area can partially offset weakness in another. A state that faces constraints in conventional military power may still exert influence through cyber operations or economic leverage (Kačmařík & Vašíček; 2024). Conversely, strong military capabilities may be complemented or complicated by vulnerabilities in information or diplomatic arenas. This interdependence creates a more flexible but also more intricate deterrence structure (Victoria, 2025).

Multi-domain deterrence enhances strategic resilience by providing states with multiple tools to respond to threats and shape adversary behavior. However, it also significantly increases complexity. With so many interconnected domains, actions in one area can quickly generate unintended consequences in another, raising the risk of miscalculation and escalation. As a result, deterrence today is no longer linear or confined, but layered, dynamic, and continuously evolving across multiple strategic spaces (Zieliński, 2025; Sasi et al., 2024; Edmond, 2022).

Sources of Strategic Instability

Despite the presence of deterrence mechanisms, the rivalry between Iran and Israel is increasingly shaped by structural sources of instability that make escalation more likely, less predictable, and more difficult to control (Khatun, 2026). These sources are closely tied to the nature of hybrid warfare and the multi-domain character of contemporary conflict.

One major source of instability is escalation through miscalculation. Because hybrid operations are deliberately designed to remain below the threshold of full-scale war, they often operate in ambiguous space where intentions and limits are not clearly defined (Genini, 2025). Actions that are intended as limited signals or calibrated pressure can easily be misinterpreted as preparations for larger or more aggressive moves. In such an environment, uncertainty about “red lines” increases the risk that both sides will overreact to perceived threats, even when no large-scale escalation was intended (Payne, 2026).

Closely related to this is the challenge of attribution. Many modern forms of conflict, particularly cyber operations and covert activities do not immediately reveal their source. When responsibility for an attack is unclear, decision-makers are forced to respond under conditions of incomplete or uncertain information (Prasad et al., 2025). This delay or misjudgment in attribution can lead to inappropriate or disproportionate responses, increasing the risk of unintended escalation.

Another important factor is the compression of decision time. The increasing use of missiles, drones, and rapid strike capabilities has significantly reduced the time available for warning, assessment, and response (Dar, 2026). Leaders may have only minutes or hours not days to interpret events and decide on a course of action. This compressed timeline increases cognitive pressure, raises the likelihood of errors, and reduces opportunities for diplomatic de-escalation.

A further source of instability lies in proxy autonomy. Both Iran and Israel have historically relied on allied non-state actors to project influence and conduct operations in regional theaters. However, these actors do not always operate under strict centralized control (Abbasi, 2025; Kausch, 2017). At times, they may act independently or pursue their own strategic or local objectives. Such semi-autonomous behavior can unintentionally escalate tensions between the sponsoring states, even when neither government initially intended a direct confrontation.

The cross-domain spillover significantly amplifies instability in the Iran-Israel rivalry. In today's interconnected strategic environment, actions in one domain can quickly trigger consequences in another. For example, a cyberattack on critical infrastructure may provoke a military response, while a maritime incident could escalate into diplomatic or kinetic confrontation (Badgi & Williams, 2025). This interdependence between domains means that escalation is rarely contained within a single sphere and can expand rapidly in unexpected directions.

Taken together, these factors illustrate why strategic stability in this context is increasingly fragile. Even when both sides seek to manage conflict and avoid full-scale war, the structural features of hybrid and multi-domain competition create persistent risks of miscalculation, rapid escalation, and unintended conflict expansion.

Why Stability Has Not Collapsed Completely

Despite the intensity and frequency of confrontation between Iran and Israel, the rivalry has not escalated into full-scale war. Instead, it has remained within a tense but generally contained form of conflict (Yilmaz & Mamouri, 2025). This outcome may appear surprising given the depth of hostility, but several important stabilizing factors help explain why complete breakdown has been avoided. One of the most important reasons is mutual vulnerability. Both states understand, at a strategic level, that an unrestricted war would carry extremely high costs. Even though they possess different military capabilities and doctrines, neither side can assume immunity from significant retaliation or broader regional escalation (Jervis, 1993; Benvenisti, 2010; Perkovich, 2022). This shared awareness of vulnerability creates a powerful incentive for restraint, even in moments of heightened tension.

Closely related to this is the practice of calibrated escalation. In most cases, both Iran and Israel tend to respond to provocations in a measured and proportional manner. Rather than pursuing maximum destruction, their responses are often designed to restore deterrence, signal resolve, and re-establish strategic boundaries (Yacoubian, 2026). This pattern of controlled retaliation helps prevent isolated incidents from spiraling into uncontrollable escalation.

External constraints also play a significant stabilizing role. Key international and regional actors, including the United States and several Gulf states, consistently exert diplomatic pressure aimed at preventing wider conflict (Ahmed & Bashir, 2026). These external actors have strong interests in regional stability, particularly because escalation could draw in multiple parties and destabilize global security environments. Their involvement often acts as a brake on further escalation.

Economic interdependence adds another layer of restraint. A major regional war would have severe consequences for global energy markets, trade routes, and investment flows, particularly in strategically important areas such as the Persian Gulf (Adrian et al., 2026). The potential disruption of these systems creates strong incentives for all involved actors to avoid actions that could trigger uncontrolled escalation.

Domestic political considerations further reinforce caution. Both Iranian and Israeli leaderships must balance external strategic objectives with internal economic conditions, political stability, and public opinion. Leaders are therefore often constrained by the need to maintain domestic legitimacy, avoid economic shocks, and prevent societal disruption, all of which discourage full-scale war (Liu, 2025).

These factors explain why strategic stability, although fragile, has not completely collapsed. Instead, it persists in a conditional and constantly managed form. The relationship is not stable in a traditional sense, but rather carefully contained through mutual restraint, external pressure, and calculated decision-making under high risk.

3.0 Implications for Strategic Theory

The evolving rivalry between Iran and Israel offers important insights that go beyond the specific regional context and speak directly to broader debates in strategic studies and international relations theory. It suggests that many long-standing assumptions about deterrence and stability need to be reconsidered in light of contemporary patterns of hybrid and multi-domain conflict.

First, the case demonstrates that strategic stability is increasingly process-based rather than condition-based. In classical theory, stability was often treated as a relatively fixed condition something achieved and maintained once a balance of power or deterrence equilibrium was established (Vander Vennet & Geeraerts, 2021). In contrast, the Iran-Israel experience shows that stability today is continuously produced and reproduced through ongoing interaction, signaling, and calibrated responses. It is less a settled state and more a dynamic process of constant management (Politics Society, 2026b). This shifts the debate from static models of containment toward a fluid framework of managed escalation, extending Kroenig's (2024) arguments on great power rivalry by showing how revisionist and status-quo powers navigate structural vulnerabilities without triggering systemic collapse.

Second, hybrid warfare simultaneously lowers the threshold for conflict while raising the threshold for full-scale war. On one hand, the availability of cyber tools, proxy forces, and limited strike options makes it easier for states to engage in hostile actions below the level of conventional war (Genini, 2025). This increases the frequency of conflict episodes. On the other hand, the same complexity and risk of escalation make states more cautious about crossing into total war, thereby raising the barrier to large-scale conventional escalation. This paradox deepens Kühn's (2023) analysis of strategic stability by demonstrating that non-linear conflict domains do not simply erode deterrence; rather, they re-channel state aggression into highly calculated, non-kinetic grey zones.

Third, deterrence in this environment increasingly depends on resilience, adaptability, and cross-domain integration. Traditional deterrence models focused heavily on military balance alone, particularly nuclear or conventional capabilities. However, the Iran-Israel case shows that effective deterrence now requires the ability to absorb shocks, respond flexibly across multiple domains, and integrate military, cyber, informational, and economic tools into a coherent strategic posture (Pivariu, 2026).

Fourth, the experience suggests that proxy-based deterrence is becoming less reliable as a long-term strategy. While proxies remain important instruments of influence, their effectiveness is increasingly limited by fragmentation, loss of centralized control, and vulnerability to countermeasures. As a result, reliance on non-state actors alone may no longer provide sufficient strategic depth or deterrent credibility in highly contested environments.

Finally, technological diffusion is fundamentally reshaping power asymmetries in international politics. The widespread availability of drones, cyber capabilities, and precision-guided munitions has lowered entry barriers to advanced forms of warfare (Pokorny, 2026b). This enables both state and non-state actors to project power more effectively, challenge stronger adversaries, and impose significant costs without requiring traditional military superiority. As a result, the distribution of power is becoming more fluid and less predictable.

This shows the Iran-Israel case highlights a broader transformation in the logic of strategy. It shows that contemporary deterrence and stability are shaped less by static balances of power and more by dynamic interactions across multiple domains, driven by technology, adaptability, and continuous strategic adjustment.

4.0 Policy Implications

The evolving strategic relationship between Iran and Israel highlights the urgent need for policymakers to rethink how stability is maintained in an era of hybrid and multi-domain conflict. Traditional tools of crisis management and deterrence, while still relevant, are no longer sufficient on their own. Instead, sustaining stability now requires an adaptive, layered approach anchored in the geopolitical realities of the Middle East.

A key priority is the establishment of functional crisis communication mechanisms. Because direct diplomatic relations between Jerusalem and Tehran are non-existent, standard hotlines are unfeasible. Instead, crisis communication must rely on institutionalized backchannels through trusted intermediaries. Neutral state actors like Oman and Switzerland which already hosts the United States' foreign interests' section in Tehran or Qatar are best positioned to serve as rapid-transmission nodes to clarify intentions and prevent miscalculations during kinetic escalations.

Equally important is the development of improved cyber norms and reliable attribution frameworks within regional gray-zone operations. Given the persistent, low-level cyber warfare targeting civilian infrastructure in both states, uncertainty over responsibility increases the risk of unpredictable retaliatory cycles. Clearer international norms, combined with third-party technical attribution from independent global bodies, would help reduce ambiguity and support more proportionate, non-escalatory responses.

Another critical area is the integration of air and missile defense architectures. As evidenced by recent direct engagements involving ballistic missiles and drone swarms, unilateral defense is insufficient. Regional stability relies on the continued expansion of integrated air defense frameworks, such as the informal coalition involving Israel, the United States, and regional Arab partners. Enhancing real-time radar data-sharing and early-warning networks across the region provides a collective deterrent that dramatically lowers the strategic utility of deep-strike saturation attacks.

Policymakers must also focus on clearer signaling of red lines. In this rivalry, excessive strategic ambiguity has repeatedly led to dangerous miscalculations. Establishing and communicating credible thresholds for response—particularly regarding the targeting of sovereign territory, diplomatic missions, or critical domestic infrastructure—can help deter provocative actions while reducing the likelihood of unintended, full-scale conventional warfare.

The protection of critical infrastructure remains an absolute policy priority. Energy systems, maritime shipping corridors, communication networks, and financial centers are prime targets in this multi-domain conflict. Strengthening their resilience through physical security, supply-chain redundancy, and robust cybersecurity measures is vital to minimizing the strategic shocks that invite severe military retaliation.

Ultimately, regional and global security frameworks must adapt to the realities of persistent, multi-domain, and deliberately ambiguous conflict. Stability between Iran and Israel can no longer be understood as the complete absence of confrontation, but rather as the capacity to manage continuous competition without allowing it to explode into regional war. This requires flexible backchannel diplomatic institutions, improved defensive coordination among international stakeholders, and a pragmatic understanding of how modern conflict unfolds across interconnected domains.

5.0 Conclusion

The rivalry between Iran and Israel captures the profound transformation of strategic stability in the age of hybrid warfare. It demonstrates that stability can no longer be understood as the simple absence of conflict. Instead, it represents a far more volatile condition in which adversaries continuously compete, signal intentions, and impose calculated costs on one another while striving to avoid escalation into full-scale, catastrophic war.

Hybrid warfare plays a fundamentally dual role in this contemporary landscape. On one hand, it can exert a stabilizing effect by offering states a calibrated menu of options such as cyber operations, proxy engagements, limited strikes, and targeted information campaigns that allow them to manage intense rivalry and vent strategic pressure without resorting to total war. On the other hand, it is inherently destabilizing; it compounds strategic ambiguity, multiplies unpredictable points of friction, and expands the pathways through which vertical escalation can occur, often entirely by miscalculation.

Admittedly, analyzing an ongoing, high-stakes confrontation presents distinct scholarly challenges. This study faces the inherent limitations of relying on unclassified, open-source

material to interpret a conflict defined by significant covert operations, attribution deniability, and state-level information control. Furthermore, while the unique geopolitical, ideological, and structural dynamics of the Iran–Israel axis offer a vivid template for modern multi-domain competition, caution must be exercised when generalizing these specific findings to other regional theaters with different alliance architectures.

Nevertheless, the central implication remains clear: strategic stability is no longer a fixed equilibrium to be achieved and preserved indefinitely. Rather, it is a dynamic, continuously negotiated balance shaped by ongoing interaction, technological adaptation, and constant recalibration between adversaries operating across fluid domains. In this sense, the Iran–Israel case is less a regional anomaly and more a preview of global trends reflecting a twenty-first-century security environment where conflict is persistent, boundaries are blurred, and stability depends entirely on managing confrontation under conditions of permanent uncertainty.

References

Abbasi, A. (2025). Proxy wars and regional instability: Israel-Iran conflict in the Middle East. *Advance Social Science Archive Journal*, 4(1), 1418–1427

Adan, M. A. (2026, March 10). *The new Iran–Israel strategic reality: From proxy war to direct confrontation*.

Adrian, T., Azour, J., Chalk, N., Gourinchas, P.-O., Kammer, A., Selassie, A. A., Srinivasan, K., & Valdés, R. (2026, March 30). How the war in the Middle East is affecting energy, trade, and finance. *IMFBlog*.

Aladhmi, M., & Abbas, S. T. (2025). Iran’s foreign policy in Syria before and after liberation from the Assad regime. *Contemporary Journal of Social Science Review*, 3(2), 3047.

Azdejković, M., Nikolić, D., & Stanojević, M. (2025, January). Hybrid warfare and information operations as contemporary threats to national and international security. *Megatrend Review*, 22(3), 189–200.

Azeroual, M., Moughraoui, F. Z., El Iysaouy, L., Mimouni, A., El Amrani, A., & El Markhi, H. (2026). Cybersecurity challenges and defense strategies for next-generation power systems. *Cyber-Physical Energy Systems*. <https://doi.org/10.1016/j.cpes.2025.10.00>

Azimi, A. (2026, March 5). Iran’s high-risk war strategy seems to centre on endurance and deterrence. *BBC News*. <https://www.bbc.com/news/articles/c93jj3gz8x0o>

Badawi, H. (2026). Iran’s dual strategy in the Middle East: Proxy warfare, nuclear ambitions, and strategic recalibration. *Güvenlik Stratejileri Dergisi*, 63–76.

Badgi, K., & Williams, L. (2026, March 3). *How will cyber warfare shape the U.S.-Israel conflict with Iran?* Center for Strategic and International Studies (CSIS). <https://www.csis.org/analysis/how-will-cyber-warfare-shape-us-israel-conflict-iran>

- Benvenisti, E. (2010, October). The law on asymmetric warfare. In *International law and armed conflict: Exploring the faultlines* (pp. 599–626). Brill.
- Bluth, C. (2025, June). *Operation Rising Lion and the long war over Iran's nuclear ambitions: History, capabilities, and strategic consequences*. <https://www.researchgate.net/publication/392707148>
- Bolt, P. J. (2025). Strategic stability in a new era. *Frontiers in Political Science*, 6, 1504361. <https://doi.org/10.3389/fpos.2024.1504361>
- Dar, A. A. (2026, April 23). *How technology is breaking crisis management in nuclear South Asia*. Defence Horizon Journal. <https://www.defencehorizon.org>
- Dolan, C. (2025, September 25). *Integrated deterrence and US defense strategy in NATO and AUKUS: An analysis of advanced technologies and multi-domain operations in alliance systems*. U.S. Department of Defense.
- Donelli, F. (2025). Maritime disruption in Yemen: The making of a hybrid Red Sea order. *Middle East Policy*. <https://doi.org/10.1111/mepo.70018>
- Edmond, C. (2022). Hybrid threats and deterrence effectiveness in Europe. *Defence Science Review*. <https://doi.org/10.37055/pno/221320>
- Fink, A. L. (2017, September 4). *Crisis stability in the twenty-first century*. University of Maryland School of Public Policy.
- Genini, D. (2025). Countering hybrid threats: How NATO must adapt (again) after the war in Ukraine. *New Perspectives*, 33(2), 122–149.
- George, A. S., Baskar, T., & Srikanth, P. B. (2024, February). *Cyber threats to critical infrastructure: Assessing vulnerabilities across key sectors*. <https://doi.org/10.5281/zenodo.10639463>
- German, T., Moustakis, F., & Liaropoulos, A. N. (Eds.). (2026). *The co-evolution of technology and warfare: Reshaping the battlefield*. Routledge. <https://doi.org/10.4324/9781003520160>
- Haider, S. A. (2026, May 13). *Cycles of deterrence: Israel, Iran, and the institutionalisation of escalation in the Middle East*. Countercurrents. <https://countercurrents.org/2026/05/cycles-of-deterrence-israel-iran-and-the-institutionalisation-of-escalation-in-the-middle-east/>
- Heiran-Nia, J. (2026, April 17). 'Unconditional escalation' marks Iran's shifting deterrence strategy. *Terrorism Monitor*, 24(7). <https://jamestown.org/unconditional-escalation-marks-irans-shifting-deterrence-strategy/>
- Hiruni, C. (2024, November). *Psychological warfare in the digital age: The role of cyber operations in modern PsyOps*. <https://doi.org/10.13140/RG.2.2.34079.37283>

Huth, P. K. (1999). Deterrence and international conflict: Empirical findings and theoretical debates. *Annual Review of Political Science*, 2(1), 25–48.

Institute for Economics and Peace. (2026). *Global Terrorism Index 2026: Special supplement – The Iran war and the global terrorism threat*. <https://www.visionofhumanity.org/wp-content/uploads/2026/03/The-Iran-War-and-The-Global-Terrorism-Threat.pdf>

Iran International. (2026, April 27). *Israel and Iran enter a phase of “implausible deniability” in their clandestine war*. <https://www.iranintl.com/en/202604270214>

Iroye, S., Ibebunjo, B. O., Fatele, S. O., & Ashibi, J. (2024, December). *Emerging trends in conflict resolution, peace and strategic studies*. Department of Peace Studies and Conflict Resolution, National Open University of Nigeria.

Jervis, R. (1993). Arms control, stability, and causes of war. *Political Science Quarterly*, 108(2), 239–253. <https://www.jstor.org/stable/2152010>

Kačmařík, O., & Vašíček, R. (2024). The multi-domain approach to military operations and its challenges to intelligence and intelligence, surveillance, reconnaissance. *Challenges to National Defence in a Contemporary Geopolitical Situation*, 1(1). <https://doi.org/10.3849/cndcgs.2024.357>

Kaprisma, H. (2020). Psychological operations: From the communication, media, propaganda, and social-culture perspective. *Jurnal Pertahanan: Media Informasi tentang Kajian & Strategi Pertahanan*, 6(2), 225. <https://doi.org/10.33172/jp.v6i2.492>

Karahalios, H. (2026). Security risks to commercial ships in the Arctic Ocean due to high tension among states. *Journal of Transportation Security*. <https://doi.org/10.1016/S18739652260000>

Kausch, K. (2017). Proxy agents: State and non-state alliances in the Middle East. *The International Spectator*, 52(1), 1–12.

Keinonen, M. (2023). Using military cyber operations as a deterrent. *International Conference on Cyber Warfare and Security Proceedings*, 18(1), 489–496.

Khan, A. (2024). Assessing the compatibility of conventional military doctrines with the changing character of war: A case of Indo-Pak rivalry. *Journal of Asian and African Studies*, 60(6). <https://doi.org/10.1177/00219096241243056>

Khatib, L. (2026, April). *The degradation of Iran’s proxy model*. Belfer Center for Science and International Affairs, Harvard Kennedy School. <https://www.belfercenter.org/research-analysis/degradation-irans-proxy-model>

Khatun, A. (2026, March). Proxy warfare and regional security dynamics: Explaining the strategic rivalry between Iran and Israel in the Middle East. *International Journal of Interdisciplinary and Multidisciplinary Research*, 11(2), 190–197. <https://doi.org/10.54121/2021111497>

- Kotait, A., & Ismail, A. (2025, April). Geopolitical threats in the Red Sea: The future of the Suez Canal amid regional and international challenges. *Scientific Journal for Commercial and Environmental Studies*, 16.
- Kroenig, M. (2024, October 7). *Strategic stability in the third nuclear age*. NATO.
- Kühn, U. (2023). Strategic stability in the 21st century: An introduction. *Journal for Peace and Nuclear Disarmament*, 6(2), 1–8. <https://doi.org/10.1080/25751654.2023.2223804>
- Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security: Emerging trends and recent developments. *Energy Reports*, 7, 8176–8186.
- Liu, S. (2025). Beyond the battlefield: Economic and geopolitical reverberations of the 2024 Israel-Iran escalation in the Middle East, South Asia, and East Africa. *Asian Journal of Middle Eastern and Islamic Studies*, 19(2), 130–153.
- Manara Magazine. (2026, April). *Israel's new military strategy in Iran*. <https://manaramagazine.org/2026/04/israels-new-military-strategy-in-iran/>
- Maulana, M. A. (2024). Unveiling Iran's deterrence by denial strategy in retaliatory strike against Israel. *Indonesian Journal of International Relations*, 8(2), 480–503. <https://doi.org/10.32787/ijir.v8i2.57>
- Mazarr, M. J. (2021). Understanding deterrence. In F. Osinga & T. Sweijts (Eds.), *NL ARMS Netherlands annual review of military studies 2020* (pp. 11–28). T.M.C. Asser Press. https://doi.org/10.1007/978-94-6265-419-8_2
- Mekelberg, Y. (2026, May). Israel and Iran enter a phase of 'implausible deniability' in their clandestine war. *Arab News Japan*.
- Mitrovic, M. (2017). Hybrid warfare and asymmetric security threats. *Vojno delo*, 69(5), 333–346.
- Morgan, P. M. (2012). The state of deterrence in international politics today. *Contemporary Security Policy*, 33(1), 85–107. <https://doi.org/10.1080/13523260.2012.659589>
- Mumford, A., & Carlucci, P. (2022). Hybrid warfare: The continuation of ambiguity by other means. *European Journal of International Security*, 8(2), 161–175.
- Na'inna, A. M., & Anti-Dwanso, V. (2022). Arms race in the 21st century: Consequences and mitigating measures. *Global Journal of Social Sciences*, 21(1), 45–65.
- North Atlantic Treaty Organization. (2024, April 24). *Countering hybrid threats*. https://www.nato.int/cps/en/natohq/topics_156338.htm
- Payne, K. (2026). *AI arms and influence: Frontier models exhibit sophisticated reasoning in simulated nuclear crises*. arXiv. <https://arxiv.org/abs/2602.14740>

- Peczeli, A. (2023, July 12). Strategic stability and the future of arms control. *per Concordiam*. <https://perconcordiam.com/strategic-stability-and-the-future-of-arms-control/>
- Perkovich, G. (2022, October 12). *Engaging China on strategic stability and mutual vulnerability*. Carnegie Endowment for International Peace.
- Pivariu, C. (2026, May 5). The Iran–U.S./Israel conflict one month after its outbreak: The logic of controlled escalation and systemic risk analysis. *Eurasia Review*. <https://www.eurasiareview.com/2026/05/05-the-iran-u-s-israel-conflict-one-month-after-its-outbreak-the-logic-of-controlled-escalation-and-systemic-risk-analysis>
- Pivariu, C. (2026). *The Iran–U.S./Israel conflict one month after its outbreak: The logic of controlled escalation and systemic risk*. International Institute for Middle East and Balkan Studies (IFIMES). <https://www.ifimes.org/en/researches/the-iran-usisrael-conflict-one-month-after-its-outbreak-the-logic-of-controlled-escalation-and-systemic-risk/5843>
- Pokorny, L. (2026, February). *The macroeconomic cost of proxy warfare: A counterfactual analysis Estimating GDP and development losses attributable to Iranian proxy activities*. <https://doi.org/10.5281/zenodo.18715206>
- Pokorny, L. (2026, March). *The economics of asymmetric attrition: A quantitative analysis of low-cost drone warfare in the Ukraine and Iranian Shahed programs (2022–2026)*. <https://doi.org/10.5281/zenodo>.
- Popalzay, A. W., Mir, M. R., & Mol, R. (2025). From proxy warfare to direct confrontation: The evolving landscape of the Israel–Iran conflict 2024–2025. *Chinese Journal of International Review*, 7(4). <https://doi.org/10.1142/S2630531325500179>
- PolSci Institute. (2025). *Proxy war: Indirect conflict and its political implications*. <https://polsci.institute/peace-conflict-studies/proxy-war-indirect-conflict-political-implications/>
- Politics Society. (2026, March 18). *The war on Iran: An analysis of the logic of conflict and potential scenarios*. <https://politicsociety.org/2026/03/18/the-war-on-iran-an-analysis-of-the-logic-of-conflict-and-potential-scenarios/?lang=e>
- Prasad, N., Diro, A., Warren, M., & Fernando, M. (2025). A survey of cyber threat attribution: Challenges, techniques, and future directions. *Computers & Security*. <https://doi.org/10.1016/j.cose.2025.10460>
- PW Live. (2026). *Iran–Israel conflict*. <https://store.pw.live/blogs/upsc-exams/iran-israel-conflict>
- Rawat, R. (2026, March 28). Beyond technology: The “way of war” in the Iran conflict – Analysis. *Eurasia Review*. <https://www.eurasiareview.com/28032026-beyond-technology-the-way-of-war-in-the-iran-conflict-analysis>

Roman, G. (2026, February 28). *Iran strike scenarios: Retaliation, transition, and the path forward*. Middle East Forum. <https://www.meforum.org/mef-reports/iran-strike-scenarios-retaliation-transition-and-the-path-forward/>

Sasi, T., Lashkari, A. H., Lu, R., Xiong, P., & Iqbal, S. (2024). A comprehensive survey on IoT attacks: Taxonomy, detection mechanisms and challenges. *Journal of Information and Intelligence*, 2(6), 455–513.

Sciarrone, M. O. (2017). *Cyber warfare: The new front*. George W. Bush Presidential Center.

Shahbazi, M., & Bunker, D. (2024). Social media trust: Fighting misinformation in the time of crisis. *International Journal of Information Management*, 75, 102780.

Shankar, P. (2026, March 2). What is Iran's military strategy? How it has changed since June 2025 war. *Al Jazeera*. <https://www.aljazeera.com/news/2026/3/2/what-is-irans-military-strategy-how-it-has-changed-since-june-2025-war>

Shapira, I. (2026, April 15). "Ultra Prevention": Israel's evolving security doctrine and the trauma of October 2023. RealClearDefense.

Suh, K. (2023). Nuclear balance and the initiation of nuclear crises: Does superiority matter? *Journal of Peace Research*, 60(2), 337–351. <https://doi.org/10.1177/00223433211067899>

Ucko, D. H., & Marks, T. A. (2020). *Crafting strategy for irregular warfare: A framework for analysis and action*. National Defense University Press.

U.S. Army. (2025, July 10). No. 25-897: *Understanding irregular warfare*. Department of the Army. <https://api.army.mil/e2/c/downloads/2025/07/10/3af1001b/no-25-897-understanding-irregular-warfare-jul-25.pdf>

Vander Vennet & Geeraerts, G. (2021, April). *The logic of balancing: Foundations of a progressive balance-of-power theory*. Paper presented at the 78th Annual Midwest Political Science Association (MPSA) Conference, Online.

Victoria, A. (2024, January). *Invisible battlefield: Systemic warfare and the future of state power*. D2D. <https://doi.org/10.5281/zenodo.17866270>

Weissmann, M. (2021). Conceptualizing and countering hybrid threats and hybrid warfare: The role of the military in the grey zone. In M. Weissmann & N. Nilsson (Eds.), *Hybrid warfare: Security and asymmetry in the 21st century* (pp. 23–42). I.B. Tauris.

Wyss, M. (2024, October). The October 7 attack: An assessment of the intelligence failings. *CTC Sentinel*, 17(9).

Yacoubian, M. (2026, March 16). *Iran's war strategy: Don't calibrate escalate*. Center for Strategic and International Studies (CSIS). <https://www.csis.org/analysis/irans-war-strategy-dont-calibrate-escalate>

Yilmaz, I., & Mamouri, A. (2025). *The ongoing war between Iran, the US, and Israel: A brief analytical assessment*. Center for Islam and Global Affairs (CIGA).

Yılmaz, C. (2026, March). Beyond the new Cold War discourse Afro-Eurasia: The political and economic impacts of the China–US rivalry on regional actors. *International Journal of Afro-Eurasian Research (IJAR)*. <https://doi.org/10.5281/zenodo.19254204>

Young, M. (2026, March 30). *Iran rewrites its war strategy*. Carnegie Endowment for International Peace. <https://carnegieendowment.org/middle-east/diwan/2026/03/iran-rewrites-its-war-strategy>

Zamin, K. A., & Nasir, A. (2026, February). *Strategic signaling and misinterpretation in Iran–Israel military posturing: A political psychology perspective*. <https://doi.org/10.5281/zenodo.18501046>

Zhao, T. (2024, July). *Political drivers of China’s changing nuclear policy: Implications for U.S.-China nuclear relations and international security*. Carnegie Endowment for International Peace.

Zieliński, T. (2025). The integration of artificial intelligence in modern deterrence: Opportunities and challenges. *Journal of Modern Science*, 64(4), 365–386.