How to cite this article:
Habibollahi, D., Nejatpour, M., & Mohammadzadeh, M. (2026). Israeli Threats Against Iran in the Pre-Attack Period: A Multidimensional Security Analysis. *Journal of Historical Research, Law and Policy, 4*(2), 1-20. https://doi.org/10.61838/jhrlp.422

Article history:
Original Research

Dates:
Submission Date: 20 August 2025
Revision Date: 04 February 2026
Acceptance Date: 12 February 2026
Pubication Date: 01 March 2026

Israeli Threats Against Iran in the Pre-Attack Period: A Multidimensional Security Analysis

1. Davoud. Habibollahi[1] : Department of Political Science, Ta.C., Islamic Azad University, Tabriz, Iran
2. Majid. Nejatpour[2*]: Associate Professor, Department of Political Science, Allameh Tabatabaei University, Tehran, Iran
3. Morteza. Mohammadzadeh[3]: Assistant Professor, Department of Political Science, Ta.C., Islamic Azad University, Tabriz, Iran

*corresponding author's email: m.nejat@iran.ir

ABSTRACT

The escalation of the Iran–Israel confrontation into direct military conflict was preceded by a prolonged period of multidimensional strategic pressure in which military, intelligence, cyber, political, economic, psychological, and regional instruments were employed below the threshold of sustained interstate war. This study aims to identify and analyze the principal dimensions and mechanisms of Israeli threats against Iran prior to the direct attack and to explain how these interconnected threats affected Iran's national-security environment. The study adopts a descriptive-analytical approach based on documentary analysis and focuses specifically on threat-related material while excluding broader historical, ideological, and security discussions that do not directly contribute to explaining the pre-attack environment. The findings indicate that Israeli threats against Iran were not limited to the possibility of conventional military strikes. Military coercion and threats against nuclear, missile, and strategic facilities interacted with intelligence penetration, espionage, targeted assassinations, sabotage, cyber operations against critical infrastructure, diplomatic and economic pressure, information warfare, and psychological influence. Intelligence activities constituted a particularly important enabling mechanism because the collection of information concerning strategic facilities, personnel, command structures, and technological vulnerabilities could facilitate covert action, cyber operations, and military targeting. The findings further demonstrate that Israel's regional relationships, particularly its strategic cooperation with the Republic of Azerbaijan, altered the geographical dimensions of the threat by increasing Iranian concerns regarding intelligence access, surveillance, military technology, and operational proximity along its northwestern frontier. The study concludes that the pre-attack period should not be interpreted as a condition of peace abruptly replaced by war. Rather, it represented an escalating hybrid confrontation in which covert, technological, political, informational, and regional pressures progressively reduced the distinction between indirect rivalry and direct military conflict. The eventual transition to overt military confrontation was therefore embedded in a security environment whose operational and strategic foundations had already developed over an extended period.

Keywords: *Iran–Israel Conflict; Israeli Threats; National Security; Hybrid Warfare; Intelligence Operations; Cyber Threats; Azerbaijan; Regional Security*

Introduction

The confrontation between Iran and Israel developed over several decades from a predominantly ideological and political rivalry into a multidimensional security conflict involving military deterrence, intelligence operations,

cyberattacks, sabotage, regional competition, diplomatic pressure, and information warfare. Understanding the Israeli attack on Iran therefore requires examining the environment that preceded direct military confrontation rather than treating the attack as an isolated event. Long before the transition to open interstate hostilities, both states had regarded the other as an important component of their respective security calculations, while their rivalry increasingly extended beyond their immediate geographical environments. Bazoobandi and Talebian's examination of the evolution of Iranian-Israeli rivalry in the Red Sea and Eastern Africa demonstrates how competition between the two states had gradually expanded geographically and strategically, becoming embedded in regional relationships beyond the traditional Middle Eastern theater (1). This geographical expansion was accompanied by changes in the instruments of confrontation. Military capabilities continued to constitute the most visible dimension of the rivalry, but intelligence gathering, covert action, cyber operations, diplomatic coalition-building, sanctions-related pressure, psychological operations, and relations with states surrounding Iran increasingly complemented conventional military instruments. In this sense, the pre-attack environment was characterized not by an absence of conflict, but by a condition in which conflict remained largely below the threshold of sustained direct interstate warfare. Gotteland's analysis of the escalation of the Iran-Israel conflict similarly situates the eventual military confrontation within a longer escalatory trajectory rather than presenting it as an abrupt rupture without strategic antecedents (2). The direct attack can consequently be understood as the most visible stage of a confrontation whose military, technological, political, and intelligence foundations had already been developing for years.

The roots of this adversarial relationship are simultaneously strategic and ideological. Since the establishment of the Islamic Republic, Iranian and Israeli political identities and regional policies have increasingly been constructed in opposition to one another. Iran's rejection of Israel's regional legitimacy, its support for Palestinian organizations and Hezbollah, and its efforts to establish political and security influence across the Middle East have been interpreted in Israel as threats to Israeli strategic interests. Israel, conversely, has been perceived by Iranian decision-makers as a militarily superior, technologically advanced, nuclear-capable state closely integrated into the strategic architecture of the United States in the Middle East. Ideological variables have reinforced these material sources of tension. Research examining Jewish messianic influences on Israeli foreign-policy hostility toward Iran identifies ideological and religious narratives as contributing factors in perceptions of Iran within Israeli strategic thinking (3). A parallel examination of Christian Zionism also argues that ideological frameworks extending beyond Israel itself have contributed to political support for confrontational policies toward the Islamic Republic (4). These ideological explanations should not, however, replace geopolitical analysis. Rather, they illuminate how material disputes over regional power, nuclear capability, military deterrence, and alliance formation have been interpreted through mutually antagonistic political narratives. The threat environment that emerged was therefore produced through an interaction between strategic interests and enduring perceptions of existential or ideological incompatibility.

A particularly important development in this rivalry was Israel's increasing representation of Iran not merely as a competitor but as a strategic security threat. Iran's nuclear program, missile capabilities, relationships with non-state armed organizations, and regional influence provided the principal material foundations for this perception. Deutsche Welle's reporting on Israeli claims regarding the scale of Iranian financial support for Hezbollah reflects the importance attached by Israeli policymakers to Iran's capacity to project influence through allied organizations outside Iranian territory (5). After the events associated with the Al-Aqsa Storm, Israeli assessments of their national-security environment became still more closely connected to the wider network of regional actors aligned

with Iran. Moghavemi's analysis of the effects of Al-Aqsa Storm on Israeli national security emphasizes the extent to which those events affected Israeli threat perceptions and strategic calculations (6). This environment increased the probability that Israeli policymakers would connect the immediate security challenges surrounding Israel to Iran's broader regional strategy. Consequently, actions directed against Iranian capabilities increasingly came to be justified within Israeli strategic discourse as preventive, preemptive, or deterrent measures designed to reduce a future danger rather than simply responses to completed Iranian military action.

At the same time, the rivalry became increasingly asymmetric in its operational methods. Physical distance between Iran and Israel complicated sustained conventional warfare but did not prevent either state from acting against the other's interests. Israel could employ intelligence operations, cyber capabilities, clandestine networks, diplomatic relationships, covert sabotage, targeted attacks, and cooperation with Iran's neighbors without engaging in continuous conventional war. The cyber domain was particularly important because it offered the possibility of imposing costs on sensitive Iranian systems without necessarily crossing the political threshold associated with an acknowledged kinetic attack. Abbasi identifies cyber operations associated with the United States and Israel as an important component of the threat environment confronting Iran and discusses Iranian counterstrategies in response to such pressures (7). Cyber operations also possessed an important strategic ambiguity: attribution could remain contested, allowing an attacker to cause economic, technical, or operational damage while complicating the targeted state's decision about whether and how to retaliate. The same logic applied to covert sabotage and intelligence operations. Where responsibility remained unofficial, a severe security incident could occur without automatically producing the diplomatic and military consequences that would normally follow an openly acknowledged interstate strike. Such mechanisms gradually blurred the distinction between peace and war.

The regional dimension was equally significant. Israeli strategy toward Iran did not depend exclusively on Israel's own geographical position. Relations with states in Iran's wider neighborhood could provide diplomatic access, intelligence opportunities, commercial links, defense cooperation, technological penetration, and a more favorable strategic environment. The development of relations between Israel and several Arab states also affected this regional balance. Arghavani Pir Salami and Arayesh interpret Arab normalization with Israel partly through a balance-of-threat framework in which perceptions of Iran contributed to regional realignment (8). Such normalization did not automatically create an operational alliance against Iran, but it weakened the assumption that Arab-Israeli antagonism would permanently prevent Israel from developing strategic relationships in Iran's regional environment. In strategic terms, this increased the number of diplomatic and security channels through which pressure on Iran could potentially be exercised. The process also reinforced Iran's perception that Israeli power was becoming increasingly embedded in the regional order rather than remaining geographically and diplomatically isolated.

The Republic of Azerbaijan occupies an especially important position within this context. Unlike Israel's relationships with more distant states, Israel-Azerbaijan cooperation concerns a country that directly borders Iran and possesses considerable significance in the South Caucasus. Abbasov and Souleimanov describe the relations among Azerbaijan, Israel, and Iran as an unusual strategic triangle shaped by security considerations, regional rivalry, energy interests, and geopolitical calculations (9). Israeli-Azerbaijani cooperation has included significant defense and political dimensions, creating concern in Tehran that a state closely connected to Israel has acquired enhanced military and intelligence capabilities immediately adjacent to Iranian territory. The significance of this relationship should not be exaggerated into an assumption that every Azerbaijani-Israeli interaction constitutes an anti-Iranian operation. Nevertheless, geographic proximity changes the security implications of cooperation.

Intelligence collection, electronic monitoring, unmanned systems, transportation networks, and security partnerships become more consequential when they operate near a target state's borders. For Iran, the northern frontier therefore became part of the wider geographical architecture of its confrontation with Israel.

The purpose of this study is to analyze the principal forms of Israeli threat against Iran during the period preceding the direct attack and to explain how apparently separate military, intelligence, cyber, political, economic, psychological, and regional pressures became interconnected. The central research question is: What were the principal dimensions and mechanisms of Israeli threats against Iran before the direct attack, and how did their interaction transform Iran's national-security environment? The study argues that the pre-attack period should be conceptualized as a stage of hybrid strategic confrontation in which Israel combined the deterrent effect of military superiority with intelligence penetration, covert action, cyber pressure, international political mobilization, regional partnerships, and psychological influence. These instruments were not independent categories. Intelligence gathering could facilitate sabotage or targeting; cyber operations could damage infrastructure while producing psychological effects; military threats could reinforce diplomatic pressure; and regional partnerships could reduce geographical barriers to intelligence collection and strategic access. The significance of the pre-attack period therefore lies in the cumulative interaction among these instruments.

Methodologically, the study adopts a descriptive-analytical approach based on documentary analysis. It draws on the conceptual and empirical material of the underlying thesis while limiting the analysis to information relevant to Israeli threats against Iran prior to direct military confrontation. Material relating primarily to general definitions of national security, unrelated historical controversies, Iranian operations against Israel, or policy questions that do not directly illuminate the Israeli threat environment is excluded. The analysis also distinguishes between established strategic relationships and contested operational claims. This distinction is particularly necessary in the intelligence domain, where publicly available evidence is often incomplete and where governments, security agencies, political actors, and media organizations may have incentives to frame incidents in conflicting ways. The objective is therefore not to present every allegation as a verified fact but to identify the structure of the perceived and demonstrated threats that shaped Iranian security calculations before the attack. Later assessments of the actual conflict reinforce the importance of examining this preceding environment. The United Nations Security Council documentation concerning the Israeli attack on Iranian nuclear facilities illustrates the eventual transition from long-standing concern about Iran's nuclear infrastructure to direct kinetic action against such targets (10), while retrospective studies of the twelve-day conflict document the human and material consequences produced once the confrontation crossed that threshold (11). The period before the attack is thus analytically important precisely because it reveals how the foundations of direct confrontation had been progressively constructed before open warfare occurred.

Theoretical and Strategic Framework of Israeli Threats Against Iran

A useful analysis of Israeli threats against Iran requires a concept of security broad enough to include military power without reducing national security exclusively to conventional military confrontation. Contemporary interstate rivalry often operates simultaneously through military, technological, economic, political, informational, and intelligence instruments. Threats can therefore originate not only from an adversary's capacity to occupy territory or destroy military forces but also from its ability to penetrate institutions, disrupt critical systems, compromise confidential information, weaken international relationships, influence domestic perceptions, or develop operational

access through neighboring states. This multidimensional conception is especially appropriate to the Iranian-Israeli rivalry because the long absence of a shared border and the political risks associated with direct war encouraged both sides to employ indirect instruments. Cyber operations offer a particularly clear example. Abbasi's analysis presents cyber threats originating from the United States and Israel as part of a larger strategic challenge to Iran rather than merely as isolated technical incidents (7). Such threats can affect industrial production, communications, financial institutions, defense systems, and public confidence simultaneously. The distinction between military and nonmilitary threats therefore becomes less rigid when nonkinetic operations can produce effects traditionally associated with physical attack.

The balance-of-threat perspective provides a useful theoretical foundation for interpreting this environment. The approach shifts attention away from aggregate power alone and toward the conditions under which one actor's power is perceived as threatening by another. Threat perception depends not only on the amount of power possessed by a state but also on geographical proximity, offensive capacity, and perceived aggressive intentions. Applied to Iran and Israel, this framework reveals why the bilateral relationship cannot be understood only through conventional measurements of military strength. Israel's sophisticated military capabilities and strategic relationship with the United States contribute to Iranian threat perceptions, but these capabilities become particularly significant when accompanied by repeated political statements regarding Iran's nuclear facilities, covert operations, intelligence activities, and regional relationships that can increase operational reach. Conversely, Israeli threat perceptions are influenced not simply by Iran's material resources but by the regional deployment of Iranian influence, missile and drone capabilities, nuclear developments, and Iran's relationships with armed groups opposing Israel. Arghavani Pir Salami and Arayesh show how regional alignments can be interpreted through precisely this logic of threat perception, particularly where Arab states' perceptions of Iran contributed to decisions concerning normalization with Israel (8). Threat is consequently relational: the same military or political capability may be interpreted differently depending on proximity, intentions, alliances, and strategic context.

Geography remains important even in an era of long-range missiles, drones, cyber operations, and satellite surveillance. Physical distance affects logistics, intelligence collection, flight routes, early warning, operational sustainability, and the political involvement of intermediary states. However, alliances and partnerships can modify the strategic meaning of distance. Israel does not share a border with Iran, but relationships with states in Iran's wider neighborhood potentially reduce some disadvantages associated with geographical separation. This is particularly evident in the South Caucasus. Abbasov and Souleimanov's analysis of Azerbaijan-Israel-Iran relations demonstrates that the triangle has acquired importance through the interaction of security, energy, and geopolitical interests (9). From a balance-of-threat perspective, therefore, Azerbaijan matters not merely because it is friendly with Israel but because cooperation takes place immediately adjacent to Iranian territory. Military technology supplied to a neighboring state, intelligence relationships near Iranian borders, and political tensions between Tehran and Baku may collectively change Iran's assessment of Israel's effective proximity. Geography in this context is not fixed; strategic relationships can effectively extend a state's reach.

Offensive capability represents another central component of the threat environment. Israel possesses advanced conventional military forces, long-range aviation, unmanned systems, missile defenses, intelligence capabilities, and sophisticated technological infrastructure. The significance of these capabilities for Iran is magnified by repeated Israeli emphasis on preventing Iranian nuclear weapon capability and by the historical use of preventive or preemptive doctrines against perceived strategic threats. During the pre-attack period, the possibility of strikes

against Iranian nuclear facilities therefore functioned as a form of coercive pressure even when no attack was immediately underway. A military threat can produce strategic effects without being implemented. It can compel the target to devote resources to air defense, dispersal, hardening, redundancy, intelligence protection, and contingency planning; it can alter investor expectations; and it can influence diplomatic negotiations by creating the possibility that failure to reach a political settlement will result in force. The later attack on nuclear facilities gives retrospective significance to these earlier signals, since the scenario long treated as a possibility ultimately became an operational reality (10). For analysis of the pre-attack period, however, the important point is that anticipated military action had already generated security consequences before direct kinetic force was used.

Perceived intention is more difficult to assess than material capability. Governments often deliberately preserve ambiguity regarding the circumstances in which they would use force, and strategic signaling may be intended simultaneously to deter, intimidate, influence allies, and shape negotiations. Israeli statements regarding Iran's nuclear program therefore cannot automatically be interpreted as evidence that a final decision to attack had already been made. Nevertheless, when rhetoric is accompanied by intelligence activity, sabotage, cyber operations, military exercises, covert action, and efforts to develop regional partnerships, the target state may reasonably interpret the combination as evidence of an increasingly serious threat. Gotteland's account of the escalation of the Iran-Israel confrontation underscores the cumulative character of the conflict and the progressive erosion of previous restraints (2). Theoretically, this suggests that threat perception is produced not by one statement or capability but by patterns. Repeated interaction can transform isolated actions into indicators of strategic intent.

The concept of hybrid threat is therefore especially useful in interpreting the pre-attack relationship. Hybrid confrontation involves the coordinated or complementary use of conventional and unconventional instruments designed to exploit vulnerabilities across several domains. In the Iranian case, military pressure represented only one layer. Intelligence networks sought access to sensitive information; cyber operations threatened digital and industrial systems; sabotage endangered infrastructure and scientific capabilities; diplomatic pressure sought to reduce Iran's international room for maneuver; economic pressure increased the material costs of confrontation; and information operations targeted perceptions inside and outside Iran. Abbasi's discussion of cyber conflict demonstrates that technological confrontation had already become integrated into the broader strategic competition between Iran, Israel, and the United States (7). Bazoobandi and Talebian similarly demonstrate that Iranian-Israeli rivalry expanded across geographical theaters, indicating that the conflict had ceased to be confined to bilateral interaction in the narrow sense (1). Together, these dynamics reveal a confrontation whose boundaries were simultaneously functional and geographical.

Intelligence should be regarded as the connective tissue among many of these dimensions. Military operations require target identification, knowledge of air defenses, information regarding command structures, assessments of vulnerabilities, and accurate timing. Cyber operations similarly depend on detailed understanding of networks, hardware, software, organizational procedures, and human behavior. Sabotage requires access, recruitment, logistics, or technical knowledge. Political and information operations are more effective when they are informed by knowledge of social divisions, institutional weaknesses, and public concerns. Consequently, intelligence penetration is not merely another threat category beside military and cyber threats. It can enable those threats. In a hybrid confrontation, intelligence advantages can produce disproportionate strategic effects because relatively small networks or technical penetrations may expose much larger systems to disruption. This is one reason why alleged Israeli intelligence activity in and around Iran has occupied such a prominent position in Iranian security discourse.

Political and ideological factors provide another layer of the framework. States do not evaluate threats through material calculation alone. Historical experience, identity, ideological commitments, and political narratives influence judgments regarding the intentions of other actors. Research on the role attributed to Jewish messianism in Israeli foreign policy argues that religious and ideological beliefs can contribute to hostile constructions of the Islamic Republic within elements of Israeli political thought (3). Studies of Christian Zionist influence similarly suggest that ideological support networks outside Israel can strengthen political approaches hostile to Iran (4). These arguments should be treated cautiously because neither Israeli politics nor Zionism constitutes a single homogeneous ideological position. Nevertheless, they help explain why Iranian-Israeli hostility has often been articulated in existential or civilizational terms that go beyond ordinary geopolitical competition. When a rival is conceptualized as fundamentally incompatible with one's political identity or national future, compromise becomes more difficult and security dilemmas become more severe.

The security dilemma is intensified when defensive and offensive measures are difficult to distinguish. Iranian missile development may be presented in Tehran as deterrence against technologically superior adversaries, while Israel may interpret the same capabilities as potential instruments of attack. Israeli intelligence and military preparations may be described in Israel as necessary preventive measures against Iran's nuclear or regional capabilities, while Iran may perceive them as evidence of aggressive intention. Each actor's attempt to improve security can therefore worsen the other's sense of insecurity. After Al-Aqsa Storm, the Israeli perception of interconnected regional threats became more acute, and Moghavemi's analysis emphasizes the event's consequences for Israeli national-security calculations (6). Iran's relationships with Hezbollah and other aligned groups further contributed to the perception that confrontation with Iran could occur indirectly through several theaters. Deutsche Welle's account of Israeli claims concerning substantial Iranian financing for Hezbollah illustrates how Israeli officials framed Iran as a source of sustained regional military pressure (5). Such perceptions encouraged Israel to treat Iranian regional influence as part of its own immediate security environment.

Economic security also belongs within the theoretical framework because sustained military and technological competition requires resources. Pressure that weakens investment, increases sanctions exposure, restricts technological exchange, or raises defense expenditure can indirectly reduce an adversary's strategic capacity. Pandin and colleagues' examination of the Israel-Iran conflict emphasizes that geopolitical confrontation can affect commodity-based investment, portfolio decisions, and broader perceptions of economic risk (12). Even before direct military action, therefore, the expectation of escalation can impose costs through uncertainty. For Iran, recurring threats against infrastructure and nuclear sites potentially increase insurance costs, discourage investment, encourage capital flight, and compel additional spending on protection. Economic pressure is thus not simply collateral to military rivalry; it may become part of the strategic environment within which the rivalry is conducted.

Finally, this theoretical framework suggests that the boundary separating deterrence from preparation for attack is inherently unstable. A state may accumulate intelligence to improve deterrence, develop cyber access for contingency purposes, strengthen alliances to increase bargaining leverage, and conduct military exercises to signal capability. Yet these same measures can also reduce the operational costs of future attack. The target state therefore confronts a fundamental uncertainty: it cannot know with confidence whether the adversary is signaling, preparing, or already conducting components of a broader operation. The pre-attack Israeli threat environment should accordingly be analyzed as an interactive system in which military capability, perceived intention, geographic access, technological penetration, and political pressure reinforced one another. This approach avoids two

analytical errors. It does not reduce every Israeli action to evidence of an inevitable predetermined war, but it also does not treat the eventual attack as disconnected from the military, intelligence, cyber, and regional patterns that preceded it.

Dimensions of Israeli Threats Against Iran Prior to the Attack

The military dimension constituted the most visible layer of Israeli pressure on Iran before the direct attack, principally because Israeli political and security discourse repeatedly centered on Iran's nuclear and missile capabilities as unacceptable strategic risks. The possibility of airstrikes against nuclear facilities remained an enduring feature of the bilateral security environment. Even where such threats were not implemented immediately, their strategic effects were substantial. Iran had to assume that facilities associated with nuclear development, missile programs, command and control, and air defense could become targets during a confrontation. This compelled investment in hardened installations, underground facilities, redundant systems, dispersal, air defense, and counterintelligence. Military pressure therefore produced costs without requiring continuous use of force. Gotteland's analysis of escalation between Iran and Israel indicates that the movement toward direct confrontation took place through successive stages in which increasingly overt military actions interacted with a preexisting shadow conflict (2). In such an environment, the threat of attack became part of strategic communication: Israel could signal that certain Iranian capabilities might eventually trigger force, while Iran could attempt to raise the expected cost of that force through deterrence and regional retaliation capabilities.

The nuclear issue intensified the coercive character of this military threat. Israeli policy has long prioritized prevention of a strategic environment in which Iran could acquire a nuclear weapons capability, while Iran has insisted on the peaceful character of its declared nuclear program. Regardless of the competing legal and political interpretations, the persistence of Israeli threats against nuclear infrastructure created a security problem for Iran that extended beyond the installations themselves. An attack on nuclear facilities could cause military escalation, environmental consequences, damage to civilian infrastructure, and a broader interstate war. The eventual Israeli attack on Iranian nuclear facilities demonstrated that these pre-attack scenarios were not purely hypothetical (10). Yet from the standpoint of the pre-attack period, the more important analytical point is that the prospect of such action already shaped strategic planning. The need to defend nuclear and missile infrastructure increased the relationship between technological security and conventional defense, making laboratories, communications systems, scientific personnel, industrial supply chains, and transportation infrastructure parts of the national-security landscape.

Targeted assassination and sabotage formed an intermediate category between conventional warfare and covert conflict. Their strategic importance derived precisely from their limited scale. A targeted operation could remove a scientist, commander, technical expert, or key capability without producing the immediate consequences associated with an acknowledged large-scale military strike. At the same time, assassination generates effects extending beyond the individual target. It communicates intelligence penetration, produces uncertainty within security institutions, imposes additional protection costs, and can disrupt scientific or military programs. It can also create psychological pressure by suggesting that physical distance, secrecy, or institutional protection cannot guarantee security. The thesis on which this article is based treats assassination threats, damage to sensitive facilities, and espionage as closely linked manifestations of the Israeli security challenge. The analytical connection among them is straightforward: successful targeting ordinarily depends on information. Intelligence concerning individuals,

routines, locations, security procedures, communications, and organizational relationships becomes operationally valuable when combined with a capacity for covert or kinetic action.

For this reason, intelligence penetration constituted one of the most consequential pre-attack threats. Israeli intelligence interest in Iran has centered on areas including the nuclear program, missile development, defense infrastructure, senior military decision-making, and strategic facilities. Intelligence operations can involve human sources, technical surveillance, communications interception, cyber penetration, satellite observation, open-source analysis, and exploitation of third-country networks. The objective is not always immediate sabotage. Strategic intelligence can improve assessments of Iranian intentions and capabilities, identify vulnerabilities, map organizational networks, and provide contingency options for future operations. In an adversarial relationship characterized by limited diplomatic communication, intelligence also substitutes for information that might otherwise be obtained through routine political interaction. Yet the same intelligence infrastructure can be used offensively. It may provide targeting information, enable sabotage, identify command nodes, or facilitate penetration of supply chains. This dual use makes intelligence activity particularly difficult to separate from preparations for coercion.

Cyber operations dramatically expanded the range of targets exposed to hostile action. Unlike conventional military attacks, cyber operations can penetrate systems without crossing borders physically and can often be conducted with uncertain attribution. Abbasi identifies Israeli and American cyber activity as a significant security challenge confronting Iran and emphasizes the development of Iranian counterstrategies in response to this threat (7). For Iran, the potential target set extends beyond military networks to electricity generation, energy infrastructure, industrial control systems, financial institutions, communications, transportation, and government databases. Operations against industrial systems are especially significant because cyber access can create physical effects. Malware introduced into control environments may disrupt machinery, alter technical processes, or damage equipment while leaving the origin of the attack uncertain. Cyber operations therefore erode the traditional distinction between digital and physical security.

The cyber threat also possesses an important psychological dimension. An attack against a major institution communicates vulnerability to the public as well as to decision-makers. If banking networks, fuel distribution, public services, communications, or industrial infrastructure become unreliable, the social effects may substantially exceed the direct technical damage. Public uncertainty about whether systems can be trusted can itself become a strategic consequence. Cyber incidents can therefore combine disruption with cognitive pressure. Abbasi's assessment of the cyber confrontation is particularly relevant because it places defensive adaptation within the broader strategic competition rather than treating cybersecurity as a narrowly technical matter (7). The need for network segmentation, indigenous technological capacity, rapid incident response, protection of industrial control systems, and counterintelligence around technical personnel consequently became part of Iran's national-security requirements before direct military conflict.

Political and diplomatic pressure represented another important component of the threat structure. Israeli policy sought to keep international attention focused on Iran's nuclear activities, ballistic missiles, regional alliances, and support for armed groups. Such diplomacy had strategic significance because successful international framing could reduce Iran's access to investment, technology, diplomatic partnerships, and economic opportunities. Pressure on third states also mattered. Where foreign governments or firms calculated that cooperation with Iran could expose them to political costs, sanctions, reputational risk, or confrontation with the United States, Israel's diplomatic influence could indirectly restrict Iranian options. The effects of political pressure therefore intersected

with economic and technological security. Iran's capacity to modernize infrastructure, procure advanced equipment, attract investment, or maintain normal financial relationships could be affected by a broader campaign to portray the country as a security risk.

Regional normalization involving Israel amplified this diplomatic dimension. The establishment and expansion of Israeli relations with Arab states demonstrated that shared or overlapping security interests could weaken longstanding barriers to cooperation. Arghavani Pir Salami and Arayesh specifically interpret normalization with Israel partly through Arab perceptions of the Iranian threat (8). From Tehran's perspective, such developments potentially transformed the regional balance by creating additional spaces for Israeli diplomatic, economic, technological, and security involvement. The importance of these relationships did not depend on the existence of a formal anti-Iran military alliance. Their strategic value could arise simply from improved access, intelligence exchange, airspace discussions, defense cooperation, or the normalization of Israeli security participation in the Gulf and wider Middle East. This progressively reduced Iran's expectation that regional opposition to Israel would automatically constrain Israel's strategic reach.

Economic pressure complemented diplomatic containment. Prolonged geopolitical confrontation creates direct and indirect financial costs even when sanctions are formally imposed by actors other than Israel. The expectation of conflict raises perceived risk; defense preparations divert public resources; restrictions on technology increase development costs; and instability can discourage foreign capital. Pandin and colleagues demonstrate that the Iran-Israel conflict has implications for commodity investment and portfolio diversification, illustrating the wider economic sensitivity of markets to geopolitical escalation (12). For Iran, the economic dimension of threat was intensified by the interaction between existing sanctions and security uncertainty. A military threat against strategic facilities could affect investor calculations even before any strike occurred. The anticipation of instability may encourage capital preservation rather than long-term productive investment and may increase pressure on exchange rates and commercial planning. Thus, military signaling can generate economic consequences without direct economic coercion.

The informational and psychological dimensions of confrontation were equally significant because modern strategic competition depends partly on control over narratives. Israel sought international support by portraying Iran as a source of regional instability, while Iranian institutions constructed Israel as an aggressive and expansionist threat. Information directed toward international audiences could influence diplomatic legitimacy, while information directed toward Iranian audiences could affect perceptions of governmental competence, military vulnerability, economic performance, and national cohesion. Social media greatly expanded the speed at which such narratives circulated. Psychological operations need not persuade citizens to adopt the adversary's worldview in order to produce effects; amplification of uncertainty, fear, distrust, or social division may itself be strategically valuable. The ideological intensity of the Iran-Israel confrontation creates particularly fertile conditions for such operations because political events can readily be interpreted through deeply established narratives of existential hostility. Studies that emphasize ideological foundations in Israeli hostility toward the Islamic Republic help explain why the rivalry is often communicated in terms extending beyond ordinary policy disagreement (3). The Christian Zionism literature similarly highlights the broader ideological networks through which hostile representations of Iran may acquire political resonance outside Israel (4).

The regional proxy dimension further complicated the distinction between direct and indirect threats. Israel viewed Iranian relationships with Hezbollah and other regional organizations as mechanisms through which Tehran

could exert military pressure without deploying conventional Iranian forces directly against Israel. Deutsche Welle reported Israeli claims that Iran supplied Hezbollah with approximately $700 million annually, illustrating the scale that Israeli authorities attributed to Iranian support (5). Whether specific estimates are accepted or contested, the strategic significance lies in Israeli perceptions of Iran's ability to project power through allied organizations. This perception encouraged Israeli action against Iranian-linked personnel, weapons transfers, and facilities outside Iran and expanded the geographical theater of competition. Bazoobandi and Talebian demonstrate that the rivalry evolved in the Red Sea and Eastern Africa as both actors sought to protect interests and limit the other's strategic position (1). Consequently, the pre-attack threat environment did not have a single geographical center. Actions in Syria, Lebanon, the Red Sea, the Caucasus, or cyberspace could influence the probability of escalation between Iran and Israel themselves.

The events following Al-Aqsa Storm further compressed this strategic environment. Israel's national-security doctrine faced intensified concerns regarding simultaneous threats from different fronts, while Iran's relationships with elements of the regional resistance network became more prominent in Israeli strategic assessments. Moghavemi argues that Al-Aqsa Storm generated important consequences for Israel's national security and altered the strategic context in which regional threats were assessed (6). As the conflict widened, the possibility that Israel would increasingly attribute regional attacks to a broader Iranian strategic architecture grew. This created an escalatory danger: the more Israel interpreted dispersed regional threats as manifestations of a single Iranian strategy, the greater the incentive to shift from attacking intermediate actors toward directly targeting Iranian capabilities. The direct confrontation that followed can therefore be understood as emerging from an environment in which indirect mechanisms were progressively losing their capacity to contain escalation.

These dimensions collectively demonstrate why the term “hybrid threat” is more analytically useful than a simple distinction between war and peace. Prior to direct attack, Iran faced the possibility of conventional military action while simultaneously confronting intelligence penetration, assassination, sabotage, cyberattacks, international political pressure, economic costs, regional coalition formation, and psychological operations. Each dimension reinforced the others. Military capability increased the coercive significance of political demands. Intelligence made military and covert operations more feasible. Cyber penetration exposed infrastructure without requiring aircraft or missiles. Regional partnerships reduced geographic constraints. Information warfare magnified the psychological effect of physical vulnerabilities. Economic pressure made the cost of prolonged strategic competition more difficult to absorb. The pre-attack Israeli threat was therefore not a collection of unrelated hostile actions but a layered strategic environment in which multiple instruments could be activated independently or combined depending on political circumstances.

Regionalization of the Israeli Threat: Azerbaijan and Strategic Encirclement

The relationship between Israel and the Republic of Azerbaijan represents one of the most strategically important regional dimensions of Iran's pre-attack threat environment because it connects Israeli military and intelligence capabilities with a state located directly on Iran's northern frontier. The strategic significance of this relationship cannot be explained simply by bilateral friendship between Baku and Tel Aviv. Azerbaijan occupies an important position in the South Caucasus, possesses significant energy resources, maintains complex relationships with Turkey, Russia, Iran, and Western states, and has pursued defense modernization partly through extensive cooperation with Israel. Israel, in turn, has developed relationships with Azerbaijan involving energy, trade,

technology, security, and military equipment. Abbasov and Souleimanov characterize the Azerbaijan-Israel-Iran relationship as an unlikely triangle in which the policies of each actor influence the strategic calculations of the other two (9). For Iran, therefore, Israeli-Azerbaijani cooperation carries implications that extend beyond normal bilateral relations because it is embedded within a competitive regional security structure.

Azerbaijan's geographic position magnifies these concerns. Israel itself is geographically separated from Iran, meaning that conventional operations require long-range capabilities, transit through or around third-country airspace, and substantial intelligence support. A cooperative relationship with a state bordering Iran does not automatically solve these operational problems, but it may alter the strategic environment by providing access to information, regional infrastructure, technical partnerships, and knowledge of developments close to Iranian territory. From a balance-of-threat perspective, this effectively modifies the variable of proximity. Israeli capability becomes more threatening to Iran when Israeli-linked technology, security relationships, or intelligence cooperation operate in neighboring territory. Abbasov and Souleimanov show that Iranian concerns regarding Israeli influence in Azerbaijan have become an important source of tension in the triangular relationship (9). Such concerns are especially sensitive because Iran's northwestern region combines strategic transportation corridors, border communities, military installations, and significant ethnic and cultural connections across the frontier.

Defense cooperation is central to this issue. Azerbaijan has become an important purchaser of Israeli military technology, including unmanned systems and other advanced defense equipment. From Baku's perspective, these acquisitions have served Azerbaijani national-security objectives, particularly in relation to the conflicts surrounding Nagorno-Karabakh and the military balance with Armenia. It would therefore be analytically inaccurate to assume that Israeli weapons supplied to Azerbaijan were acquired primarily for use against Iran. Nevertheless, the accumulation of advanced Israeli-origin technology in a neighboring state affects Tehran's security calculations. Systems capable of intelligence, surveillance, reconnaissance, precision targeting, electronic warfare, or unmanned operations may possess strategic relevance beyond the conflict for which they were originally procured. The concern is consequently based on capability and access rather than on the assumption that Azerbaijan necessarily intends military confrontation with Iran. The triangular dynamics analyzed by Abbasov and Souleimanov illustrate precisely this problem: cooperation that Baku and Tel Aviv may define according to their own bilateral interests can simultaneously be interpreted by Tehran through the lens of vulnerability and encirclement (9).

The intelligence dimension is more sensitive because public evidence concerning clandestine operations is necessarily incomplete. Iranian political and security discourse has repeatedly expressed concern that Israeli intelligence services could exploit Azerbaijani territory, contacts, or infrastructure for observation and operations directed toward Iran. Such allegations require careful qualification because intelligence cooperation is rarely documented publicly in sufficient detail to establish the operational role of specific sites or actors conclusively. Nevertheless, the strategic logic underlying Iranian concern is understandable. Intelligence organizations seek proximity to targets, access to transportation networks, linguistic and cultural knowledge, communications infrastructure, and opportunities for recruitment. A neighboring country with strong relations with the intelligence service's home state may therefore possess potential value even without serving as a formal operational base. The relevance of Azerbaijan to Israeli intelligence strategy should accordingly be analyzed in terms of opportunity structures rather than categorical assertions regarding every alleged covert activity.

This intelligence concern interacts directly with Iran's vulnerability to assassination and sabotage. If an adversary seeks information regarding sensitive personnel, nuclear facilities, missile infrastructure, supply chains, or

command networks, neighboring territories may provide useful logistical environments for observation, transit, communications, or contact with intermediaries. Intelligence operations do not necessarily require permanent bases; commercial networks, transportation routes, temporary locations, diplomatic channels, contractors, technical systems, and human relationships may all contribute to collection. The pre-attack threat therefore arose partly from uncertainty. Iranian security authorities could not assume that conventional border protection alone would prevent penetration because relevant operations might involve electronic surveillance, cyber access, recruited individuals, or transnational logistics rather than armed border crossings. This problem becomes especially significant when intelligence activity is connected to a broader pattern of covert competition.

The South Caucasus also matters because geopolitical change following the conflicts between Azerbaijan and Armenia altered the regional balance. Azerbaijan's improved military position increased its strategic confidence, while Turkey's close relationship with Baku strengthened transregional connections between the South Caucasus and the wider Middle East. Iran has generally opposed changes in internationally recognized borders that could threaten its direct access to Armenia or substantially alter regional transit arrangements. Israeli relations with Azerbaijan therefore became intertwined in Iranian perceptions with wider concerns about transportation corridors, Turkish influence, Western access, and the changing postwar order in the Caucasus. Not every component of these developments was caused by Israel, and treating the entire South Caucasus as an Israeli strategy would exaggerate Israeli agency. Yet Israel benefited from an environment in which a strategically important partner on Iran's border became militarily stronger and more regionally influential. This interaction between local conflict and external rivalry demonstrates how the Iran-Israel confrontation could be regionalized without either state directly controlling all of the actors involved.

Energy interests also provide a structural foundation for Israel-Azerbaijan relations. Azerbaijan has been a significant energy supplier and occupies a strategic position in routes connecting Caspian resources to international markets. This gives Israel an incentive to maintain stable relations with Baku independent of Iran. The existence of autonomous economic motives is important because it helps explain the durability of the relationship. Cooperation based only on hostility toward a third state may fluctuate rapidly, whereas energy, trade, and technological relationships create institutional and commercial interests that can sustain political ties over time. Abbasov and Souleimanov emphasize this interaction of energy and security within the Azerbaijan-Israel-Iran triangle (9). From Iran's perspective, however, economic cooperation can indirectly support a larger security relationship by creating frequent official contact, infrastructure, trust, and long-term strategic interdependence. Economic and security dimensions therefore need not be mutually exclusive.

The growing Israeli presence in Iran's broader regional environment should also be considered alongside normalization trends in the Arab world. The strategic concern for Tehran was not simply that one neighboring or nearby state had developed relations with Israel, but that the political cost of overt cooperation with Israel was declining across several parts of the region. Arghavani Pir Salami and Arayesh argue that perceptions of an Iranian threat contributed to Arab choices regarding normalization with Israel (8). Azerbaijan represents a different historical and geopolitical case, but the combined pattern has similar implications: Israel's regional access increasingly depends on overlapping bilateral interests rather than on a single alliance structure. Energy cooperation may motivate one relationship, shared threat perceptions another, technological exchange a third, and American strategic influence another. The result can nevertheless be a network of relationships that expands Israel's diplomatic and security reach around Iran.

The concept of strategic encirclement should consequently be used with analytical caution. There is insufficient basis for treating every Israeli regional relationship as part of a centrally coordinated plan to surround Iran geographically. Such a claim would oversimplify the independent interests of Azerbaijan, Gulf states, Turkey, the United States, and other actors. A more defensible interpretation is that Israel has benefited strategically from the expansion of relationships with states located in Iran's wider environment and has used those relationships to reduce its own diplomatic isolation, improve security cooperation, and constrain Iranian regional influence. For Iran, the cumulative effect can nevertheless resemble encirclement because Israeli political, military, intelligence, or technological presence appears in multiple neighboring or nearby theaters. The subjective perception of encirclement can itself influence security policy even when the relationships producing it have different origins.

The ethnic dimension of the Iranian-Azerbaijani relationship further increases the sensitivity of Israeli involvement. Large Azerbaijani-speaking communities live in northwestern Iran, while cultural and linguistic relationships extend across the international border. Under normal conditions, such connections can support trade, tourism, cultural exchange, and regional stability. Under conditions of interstate tension, however, nationalist narratives can become politically sensitive. Iranian authorities have periodically feared external attempts to exploit ethnic identities for separatist or destabilizing purposes. The presence of Israeli-Azerbaijani strategic cooperation can therefore be interpreted through a domestic-security lens as well as a foreign-policy lens. The relevant threat is not ethnic identity itself, nor should Azerbaijani-speaking Iranian citizens be securitized as a population. Rather, the concern lies in the possibility that external information operations could instrumentalize existing identities, grievances, or political controversies. Such operations may attempt to deepen mistrust between communities and the state even where genuine separatist support remains limited.

Information warfare can amplify this vulnerability because social media allows narratives generated outside Iran to circulate rapidly inside the country. Messages concerning ethnic discrimination, border disputes, regional history, economic inequality, or relations with neighboring states may be promoted organically, strategically, or through a mixture of both. Attribution is difficult, making it inappropriate to label all critical or nationalist content as foreign manipulation. Yet a sophisticated information strategy does not need to fabricate every grievance; it can selectively amplify real controversies and connect them to broader political narratives. The same principle applies to economic problems, corruption, environmental disputes, and dissatisfaction with public administration. Hybrid influence seeks leverage in existing social conditions rather than necessarily creating them from nothing. In this way, regional rivalry intersects with domestic resilience.

Cyber capabilities can also acquire a regional dimension. Technical infrastructure does not respect political borders in the same way as conventional armed forces. Operations may be routed through servers in multiple countries, carried out by dispersed groups, or supported by commercial and criminal networks. Abbasi's analysis of cyber threats from Israel and the United States demonstrates that Iran has had to treat cybersecurity as a strategic national-security problem (7). Proximity may still matter because regional technical cooperation, communications systems, intelligence partnerships, and human networks can support collection or operational preparation. The interaction of cyber activity with regional intelligence relationships therefore creates a threat environment in which attribution becomes especially complex. Iran may know that an operation serves Israeli strategic interests while remaining unable to determine publicly the exact role played by a neighboring state, private actor, foreign intelligence service, or proxy cyber group.

The broader geographical expansion of Iran-Israel competition confirms that this regionalization was not limited to Azerbaijan. Bazoobandi and Talebian document the evolution of competition in the Red Sea and Eastern Africa, demonstrating that both states sought influence in spaces far beyond their own territory (1). This is important because it reveals a general strategic pattern. Iran and Israel increasingly attempted to influence the other's security environment indirectly by cultivating relationships with governments, armed organizations, commercial actors, or strategic partners in third regions. Azerbaijan is distinctive primarily because of its immediate proximity to Iran and the depth of its defense relationship with Israel. The South Caucasus therefore represents the clearest example of how a geographically distant Israeli threat could be translated into a security concern at Iran's border.

Regionalization also affected deterrence. If Iran believed that Israel could obtain intelligence or operational support from locations near Iranian territory, Tehran would have to allocate additional resources to northern border security, counterintelligence, electronic defense, surveillance, and diplomatic management of relations with Baku. These measures impose opportunity costs even in the absence of confirmed hostile operations. At the same time, excessively securitized Iranian responses could worsen relations with Azerbaijan and thereby create precisely the environment in which Baku would have stronger incentives to deepen cooperation with Israel. This illustrates a classic security dilemma: Iranian attempts to reduce Israeli influence could be interpreted in Azerbaijan as pressure or hostility, encouraging Azerbaijan to seek further external security partnerships, which would then increase Iranian concern. Managing this triangle therefore required more than military deterrence.

The ultimate strategic significance of Azerbaijan in the pre-attack period lies in the interaction among geography, intelligence, technology, and political perception. Israeli-Azerbaijani relations did not make direct Israeli attack inevitable, nor is there sufficient basis to attribute all regional tensions to Israeli strategy. Nevertheless, the relationship reduced the degree to which Iran could regard Israel as a distant adversary whose operational capabilities were geographically constrained. The possibility of intelligence collection near Iran's borders, access to regional networks, advanced Israeli military technology in Azerbaijan, and recurring political tensions between Tehran and Baku collectively increased uncertainty in Iranian strategic planning. When combined with cyber threats, covert operations, military signaling, and broader Israeli normalization across the region, this relationship contributed to a multilayered perception of strategic pressure. It therefore serves as a particularly revealing case of how indirect regional partnerships became integrated into the wider structure of Israeli threats against Iran before direct military confrontation.

Conclusion

The analysis demonstrates that Israeli threats against Iran before the direct attack were multidimensional, cumulative, and increasingly interconnected. They cannot be adequately explained through the conventional image of two states standing at the threshold of military war and relying solely on missiles, aircraft, and armed forces to deter one another. The pre-attack confrontation was already active across numerous domains. Military threats created continuous uncertainty regarding the security of nuclear, missile, military, and strategic infrastructure. Intelligence activity sought information about capabilities, personnel, organizations, and vulnerabilities. Covert operations and sabotage created the possibility of inflicting strategic damage while maintaining ambiguity about responsibility. Cyber operations expanded the potential target set to include critical infrastructure and information systems. Diplomatic activity attempted to limit Iran's international room for maneuver. Economic pressure magnified the cost of strategic competition. Information and psychological operations sought to shape international

perceptions and exploit domestic vulnerabilities. Regional partnerships reduced the significance of geographical distance. These instruments collectively formed a security environment that existed below the threshold of sustained direct war but was considerably more adversarial than conventional peace.

The central objective of this study was to determine the principal dimensions and mechanisms of Israeli threats against Iran during this pre-attack period and to explain how they affected Iran's national-security environment. The analysis indicates that the most important feature was not any single category of threat but the interaction among categories. Military power became more significant when supported by accurate intelligence. Intelligence penetration became more dangerous when it could facilitate assassination, sabotage, cyber operations, or military targeting. Cyber operations acquired strategic importance when they could produce physical damage or undermine confidence in critical services. Diplomatic pressure became more consequential when combined with economic restrictions and the possibility of military escalation. Regional partnerships became more threatening when they provided potential opportunities for intelligence collection, technological cooperation, logistical access, or strategic pressure close to Iranian territory. The threat environment was therefore systemic rather than compartmentalized.

This finding changes the meaning of the term “pre-attack period.” Chronologically, it refers to the time before direct Israeli military action against Iran. Strategically, however, it should not be interpreted as a period before conflict. Conflict was already occurring, but through mechanisms designed to remain below or around the threshold of overt interstate warfare. The intelligence contest, cyber operations, sabotage, proxy confrontation, political pressure, and regional competition constituted forms of strategic interaction through which both sides attempted to constrain the other without accepting the full costs of conventional war. The eventual direct attack represented a change in the mode and intensity of confrontation rather than the creation of a wholly new conflict. This distinction is essential because it explains why military escalation could occur relatively rapidly once previous restraints weakened. Much of the informational, technological, organizational, and political infrastructure necessary for confrontation had already been developing.

Military threat played an especially important role in this process because it provided the coercive background against which other forms of pressure operated. Repeated discussion of possible attacks on strategic facilities forced Iran to treat military action as a realistic contingency. The consequence was not limited to expenditure on air defense. Threatened attack affects the location and construction of facilities, the protection of scientific and military personnel, communications security, operational secrecy, command structures, emergency planning, investment decisions, and diplomatic strategy. Military pressure therefore penetrates multiple sectors of national life before a missile is fired. The potential for attack can itself function as an instrument of coercion by raising the costs associated with continuing policies opposed by the threatening state.

Intelligence activity represented an even more fundamental challenge because it reduced the protective value of secrecy and geographical depth. A state may possess powerful armed forces and hardened facilities while remaining vulnerable if an adversary can obtain precise information concerning personnel, systems, communications, locations, routines, and organizational weaknesses. Intelligence penetration can also amplify every other form of threat. Accurate information improves targeting, supports sabotage, facilitates cyber access, reveals political divisions, identifies supply-chain vulnerabilities, and enables psychological operations. In this sense, intelligence is not simply one component of hybrid confrontation; it is one of the mechanisms that allow the separate components to function together. The pre-attack security environment therefore placed counterintelligence at the center of Iran's broader defense requirements.

Cyber operations further transformed the meaning of strategic depth. Physical distance, mountains, air defenses, and borders provide limited protection against attacks transmitted through digital networks. The cybersecurity of electricity systems, industrial facilities, financial services, communications, transportation, governmental databases, and defense infrastructure consequently became inseparable from national security. The cyber domain also complicated deterrence because attribution could remain uncertain and because responses to cyberattacks involved different political calculations from responses to conventional bombing. An operation could be severe enough to cause substantial damage yet ambiguous enough to complicate retaliation. This ambiguity gave cyber instruments particular value within the pre-attack environment, where both sides sought means of imposing costs without necessarily triggering unrestricted war.

Political and economic pressure reinforced these security challenges by increasing the long-term costs of confrontation. The international isolation of a state can restrict technology, financing, industrial cooperation, and access to global markets, thereby affecting its ability to sustain both economic development and military modernization. At the same time, military insecurity can discourage investment and shift public resources from productive sectors toward defense and protection. The relationship between economic vulnerability and strategic vulnerability is therefore reciprocal. A weaker economic foundation reduces the resources available for resilience, while persistent security threats impose additional economic burdens. For Iran, the long-term challenge was consequently not only how to prevent physical attack but how to maintain national capacity under conditions of prolonged political, technological, and security pressure.

The psychological and informational dimensions likewise demonstrate why national resilience cannot be reduced to military capability. A society experiencing repeated reports of sabotage, assassination, cyber penetration, military threats, and international pressure may develop a heightened perception of insecurity even when daily life continues normally. If citizens believe that sensitive institutions can be penetrated or that the state cannot reliably protect infrastructure, confidence may decline. External information operations can exploit these perceptions, particularly when they interact with genuine economic or political grievances. Effective national security therefore depends not merely on suppressing hostile narratives but on reducing the vulnerabilities that make those narratives persuasive. Public confidence is more sustainable when it is supported by institutional competence, reliable services, transparent communication, social inclusion, and credible crisis management.

The examination of Azerbaijan shows how regional partnerships can alter the geography of an interstate rivalry. Israel and Iran do not share a border, but strategic cooperation between Israel and a state neighboring Iran reduces the extent to which physical distance can be treated as protection. Azerbaijan's own motivations are independent and cannot simply be reduced to Israeli interests. Its defense procurement, energy relationships, foreign policy, and regional ambitions arise from its own national calculations. Nevertheless, close Israeli-Azerbaijani cooperation creates an objective security consideration for Tehran because military technology, intelligence relationships, communications networks, and political access located near Iran possess greater potential relevance than equivalent cooperation in distant regions. The resulting triangular relationship illustrates the complexity of modern security competition, in which a bilateral rivalry becomes embedded in the independent interests of third states.

This regional dimension also demonstrates the danger of excessive simplification. Treating every Azerbaijani action as part of an Israeli strategy would obscure Baku's autonomy and could encourage policies that increase rather than reduce Iranian insecurity. At the same time, dismissing the strategic significance of Israeli influence in a neighboring country would ignore the importance of geography, intelligence access, and defense cooperation. A

more effective analytical approach recognizes both realities. Azerbaijan pursues its own interests, but those interests can produce relationships that Israel may use to strengthen its regional position. Iran must therefore distinguish between legitimate bilateral cooperation among neighboring states and activities that create concrete threats to Iranian security.

The broader pattern of Israeli regional relationships produces similar conclusions. Strategic pressure does not require a formal alliance specifically organized to attack Iran. A network of separate partnerships can produce cumulative effects even when each relationship has different motivations. Diplomatic normalization can provide legitimacy; technology agreements can create institutional links; defense cooperation can improve interoperability; energy relationships can produce long-term strategic interdependence; and intelligence cooperation can expand knowledge of regional developments. From the perspective of a state attempting to assess threat, the combined consequences may be more important than the formal labels attached to the relationships. This helps explain why Iran increasingly interpreted Israeli regional integration as part of its own security environment.

The transition from indirect to direct confrontation ultimately revealed the limits of maintaining prolonged strategic competition below the threshold of war. Hybrid instruments may delay direct military conflict, but they can also produce cumulative escalation. Each assassination, cyberattack, sabotage incident, regional military development, or proxy confrontation can alter perceptions of credibility and restraint. A state that believes its adversary is gradually improving its position may conclude that delaying action will make future circumstances less favorable. At the same time, successful covert operations may encourage risk-taking by creating confidence that escalation can be controlled. The danger is that incremental measures intended to impose limited costs can eventually undermine the political and psychological barriers that previously prevented direct attack.

The principal conclusion of this study is therefore that the Israeli threat against Iran before the attack should be conceptualized as an integrated hybrid strategic environment rather than a collection of discrete incidents. Military coercion, intelligence operations, cyber pressure, sabotage, assassination, diplomatic action, economic pressure, information warfare, and regional partnerships formed mutually reinforcing layers. Their cumulative effect was to narrow the practical distance between covert rivalry and overt war. Intelligence activities developed knowledge that could support future operations; regional relationships expanded access; technological confrontation identified vulnerabilities; military signaling maintained coercive pressure; and political narratives increased the perception that the rivalry concerned fundamental national-security interests rather than negotiable policy disagreements.

Understanding this pre-attack environment is essential for interpreting the subsequent transition to direct military confrontation. The attack was significant because it crossed an important threshold, but the strategic confrontation did not begin when that threshold was crossed. Its foundations had already been constructed through years of multidomain rivalry. The most important lesson is therefore analytical rather than predictive: contemporary interstate war may be preceded by a prolonged period in which many functions traditionally associated with warfare are already being performed through covert, technological, economic, informational, and regional instruments. Recognizing this continuum makes it possible to understand how two states can formally remain outside sustained direct war while simultaneously operating within an increasingly militarized security relationship. In the Iranian-Israeli case, the pre-attack period represented precisely such a condition, and the convergence of its multiple threat dimensions created the strategic environment from which direct confrontation ultimately emerged.

Acknowledgments

We would like to express our appreciation and gratitude to all those who helped us carrying out this study.

Authors' Contributions

All authors equally contributed to this study.

Declaration of Interest

The authors of this article declared no conflict of interest.

Ethical Considerations

All ethical principles were adhered in conducting and writing this article.

Transparency of Data

In accordance with the principles of transparency and open research, we declare that all data and materials used in this study are available upon request.

Funding

This research was carried out independently with personal funding and without the financial support of any governmental or private institution or organization.

References

1. Bazoobandi S, Talebian H. The evolvement of Iran-Israel's rivalry in the Red Sea and Eastern Africa. Asian Journal of Middle Eastern and Islamic Studies. 2023;17(4):341-55.
2. Gotteland M. Escalation of the Iran-Israel Conflict. Jceeas. 2025;4(3-4):74-97. doi: 10.12700/jceeas.2024.4.3-4.252.
3. Godarzi M, Monavari SA, Karimi G. The Role of Jewish Messianism in Israel's Hostile Foreign Policy towards the Islamic Republic of Iran. Political Strategic Studies. 2022;11(42):111-45.
4. Khodāverdi M, Monavari SA, Karimi GR. The Role of Christian Zionism in Israel's Hostile Foreign Policy towards the Islamic Republic of Iran. Strategic Political Studies. 2022;11(42):111-45.
5. Deutsche W. Israel: Iran Gives Hezbollah in Lebanon $700 Million Annually. Deutsche Welle. 2023.
6. Moghavemi AR. Analyzing the Impacts of Al-Aqsa Storm on Israel's National Security. Strategic Environment Journal of the Islamic Republic of Iran. 2024;8(1):9-48.
7. Abbasi USA. Cyber Threats to Iran From USA and Israel: Counter Strategies by Iran. Global Strategic and Securities Review. 2024;IX(I):44-56. doi: 10.31703/gsssr.2024(ix-i).04.
8. Arghavani Pir Salami F, Arayesh H. The Arabs and Choice in a Threat Balance Condition; Iran's Threat Perception and Normalization with Israel. Quarterly Journal of Foreign Relations. 2022;14(4 (56)):1-25.
9. Abbasov N, Souleimanov E. Azerbaijan, Israel, and Iran: An Unlikely Triangle Shaping the Northern Middle East. Middle East Policy. 2022;29(1):139-53. doi: 10.1111/mepo.12611.
10. UNSC. Report on the Israeli attack against Iranian nuclear facilities. New York: United Nations, 2025.
11. Shaker Arani MJ, Kadivar A. Fire at Home: Re-reading Israel's Twelve-Day War Against Iran with a Focus on Martyr Statistics. Daghigheh Analytical Magazine. 2025.
12. Pandin MYR, Nurrochmah A, Rahmawati S. Implications of the Israel - Iran Conflict on Commodity-Based Investment and Portfolio Diversification. Jea17 Jurnal Ekonomi Akuntansi. 2024;9(2):32-42. doi: 10.30996/jea17.v7i2.12230.