ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.04 No.01 (2026)

HYBRID WARFARE AND REGIONAL POWER COMPETITION: A CASE STUDY OF THE 2026 IRAN–ISRAEL CONFLICT

Akhlaque Ahmed Kubar
Lecturer GDC Thari Mirwah
Ph.D scholar IR department shah Abdul latif university Khairpur
akfaroqi@gmail.com

Anees Ur Rehman (Corresponding Author)
Master of Arts in History, Ghazi University, Dera
Ghazi Khan, Pakistan
aneesurrehman094@gmail.com
Dr. Himad Ali
PhD in World History
Institute of Middle Eastern Studies (IMES)
Northwest University, Xi'an, Shaanxi Province, China
Research Fellow
Shaanxi Institute of International Studies (SXIIS)

Abstract
The Iran 2026 Israel conflict is a watershed event in the modern geopolitics as a vivid example of hybrid warfare approaches combined with rivalry on the power level in the region. This paper explores the ways state and non-state actors used a multidimensional scale of conventional military actions, cyber warfare, proxy conflicts, information attacks and nuclear coercive communications to promote strategic goals without necessarily entering into the full-scale conventional military conflicts. This qualitative case study is based on the hybrid warfare theory and regional power rivalry frameworks as it reviews secondary data comprising of peer-reviewed literature, policy reports, credible news materials published during and after the war. The results show that the Iran-Iran 2026 military conflict was not a singular military incident but the conclusion of a cycle of escalation of the decades long period or a period where a proxy war had evolved into a kinetic war. The conflict also revealed the focal role of technological asymmetry especially in the drone warfare, cyber operations and precision-strike capabilities in the development of modern regional power relations. This research adds to the existing literature on the subject of hybrid warfare by determining some peculiarities of engagement peculiar to the Middle East geopolitical situations.
Keywords: *Hybrid warfare, Iran Israel war, power rivalry in the region, proxy warfare, cyber warfare, nuclear blackmail, Middle East politics, asymmetric warfare.*

1. INTRODUCTION

The Middle East has always been typified by intricate interplays of state rivalry, non-state armed, ideological and great-power interventions. Among the most significant bilateral enmities of the post-Cold War period, in this turbulent regional formation, there is the Iran-Israel rivalry. Starting as the competition under the veil of camouflage following the Islamic Revolution of 1979, the strategy was slowly transformed into one of the most complex forms of hybrid warfare that is ever recorded in the recent literature of international relations (Hoffman, 2007; Kofman and Rojansky, 2015).

Hostilities between Israel and Iran that developed between 2023 and 2026 can provide a one-of-a-kind analytical lens by which scholars and policymakers can consider the structural dynamics of hybrid warfare in a power competition scenario in the region. Starting with the Hamas-sponsored October 7, 2023 attacks on Israel and the ensuing Gaza War, a series of escalatory measures ensued - leading to the June 2025

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.04 No.01 (2026)

Twelve-Day War, the US-Israeli strikes against the Iranian military and political leadership on February 2026 and the subsequent series of asymmetric confrontations (CFR, 2026;

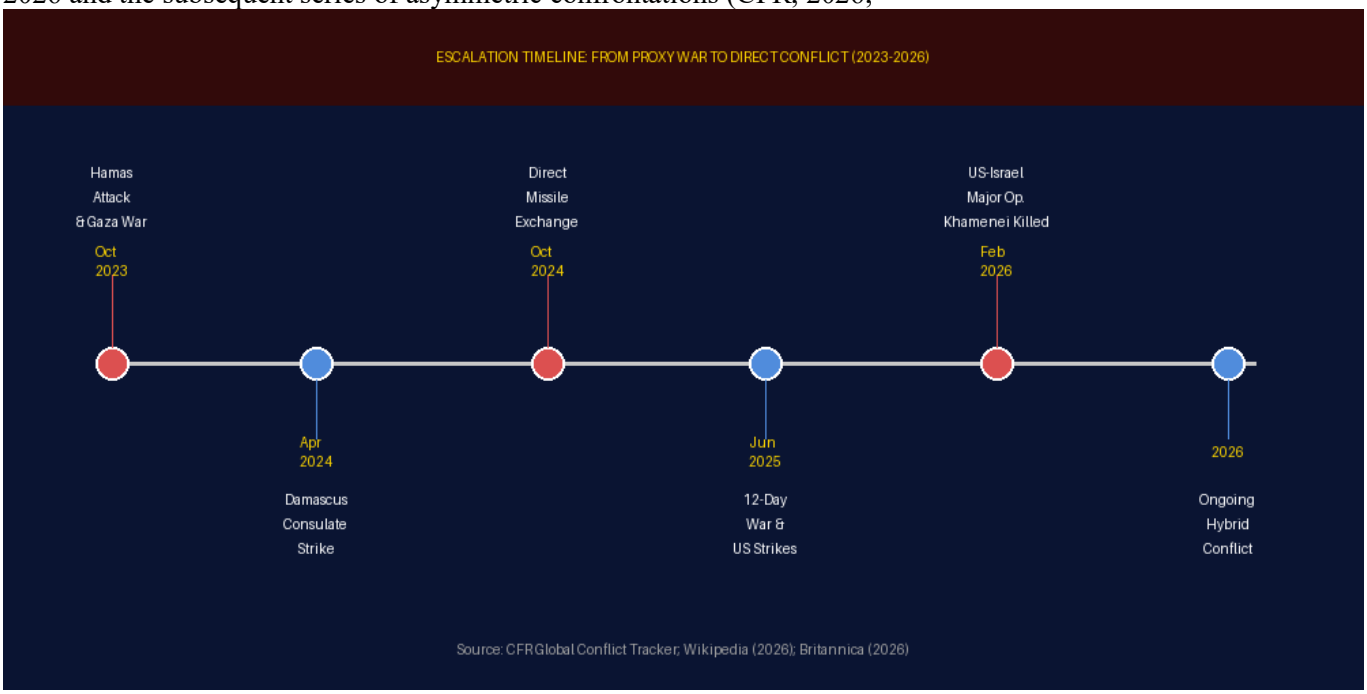


Figure 1: Iran-Israel conflict Escalation Timeline (2023-2026). Reference: The compilation of the author based on the CFR, Wikipedia, and Britannica (2026).

The 2026 Iran-Israel dynamic cannot be sufficiently explained using the traditional interstate conflict paradigms. The war was not categorized into war and peace, but a combination of covert actions of intelligence, open military attacks, cyber-attacks, proxy mobilization, economic warfare, and information campaigns to a low-level conflict that was constantly evolving (Renz, 2016; Johnson, 2018). Such a hybrid nature is akin to what scholars are more and more calling the so-called grey zone - a competitive space that intentionally pursues the space between the line of conventional war but still makes a substantial strategic impact (Mazarr, 2015).

The ideological adherence to resist Zionism, the desire to establish hegemony in the region, the creation of nuclear and ballistic missile systems as a deterrent factor have formed the strategic position of Iran (Chubin, 2009; Takeyh, 2021). Israel on the other hand has been following a forward defense policy, pre-emptive warfare, back door operations and technological excellence as counter to existential threats. Asymmetry of traditional military power has driven both the actors to adopt the hybrid strategies - Iran massively depending on proxy forces and deniable operations, whereas Israel relied on the high level of cyber capabilities, precision attacks and intelligence penetration (Eisenstadt and Knights, 2014).

The theory of hybrid warfare, which is theorized by Hoffman (2007), means the combination of traditional weapons, unusual tactics, terrorism, and disruptive technology to meet political goals. This framework should be expanded in the Iran-Israel case to include the involvement of nuclear coercive signaling, proliferation of drones and the utilization of social media as psychological battlefields (Lind et al., 1989; McCulloh and Johnson, 2013). The 2026 war is therefore an excellent source of empirical data to continue the development of hybrid warfare theory, which was mainly dominated by NATO-based perspectives.

The research question that this study will deal with is as follows: How do the dynamics of Iran-Israel conflict in 2026 depend on the hybrid warfare strategies and what do these dynamics demonstrate about the patterns of competition among the regional powers in the modern Middle East? The rest of the article goes on in the following way. Part 2 summarizes the theoretical and empirical research on hybrid warfare and power rivalry on the regional level. The qualitative methodology used is described in section 3. The

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.04 No.01 (2026)

thematic analysis of findings is presented in section 4. Section 5 will discuss theory and policy implications and finally, Section 6 will give recommendations.

What makes this study important is that it does not only provide an empirical input towards the comprehension of a particular geopolitical crisis but, also, it is theoretically significant to the larger questions regarding the nature of warfare in the twenty-first century. With hybrid approaches increasingly becoming the new form of great and regional power rivalry, the analytical tools derived in this paper are applicable in learning similar conflicts in Eastern Europe, Southeast Asia, and others (Berzins, 2014; Galeotti, 2016; Hoffman, 2009).

2. LITERATURE REVIEW

The study of hybrid warfare has grown in size since Hoffman originalized the concept in 2007. Hoffman described hybrid warfare as the merging of traditional capabilities, irregular tactics, criminal acts and terrorist acts in the same battlefield often carried out by the same groups. Later researchers have narrowed down on and challenged this definition, and some have concentrated on the psychological and informational aspects (Renz, 2016), while others have concentrated on the effect of proxy forces and plausible deniability (Kofman and Rojansky, 2015).

Murray and Mansoor (2012) consider that hybrid warfare is not a recent occurrence but a recurring aspect of war over the years with the modern versions being characterised by their level of technological advancement and the complexity of information. Such historical approach is especially applicable in the case of the Iran-Israel conflict, which has possessed the features of hybridity during various decades - since the Stuxnet cyberattack of 2010 carried out by Israel and the United States to the mobilization of the Hezbollah proxies during the 2006 Lebanon War and the further (Lindsay, 2013; Blanford, 201

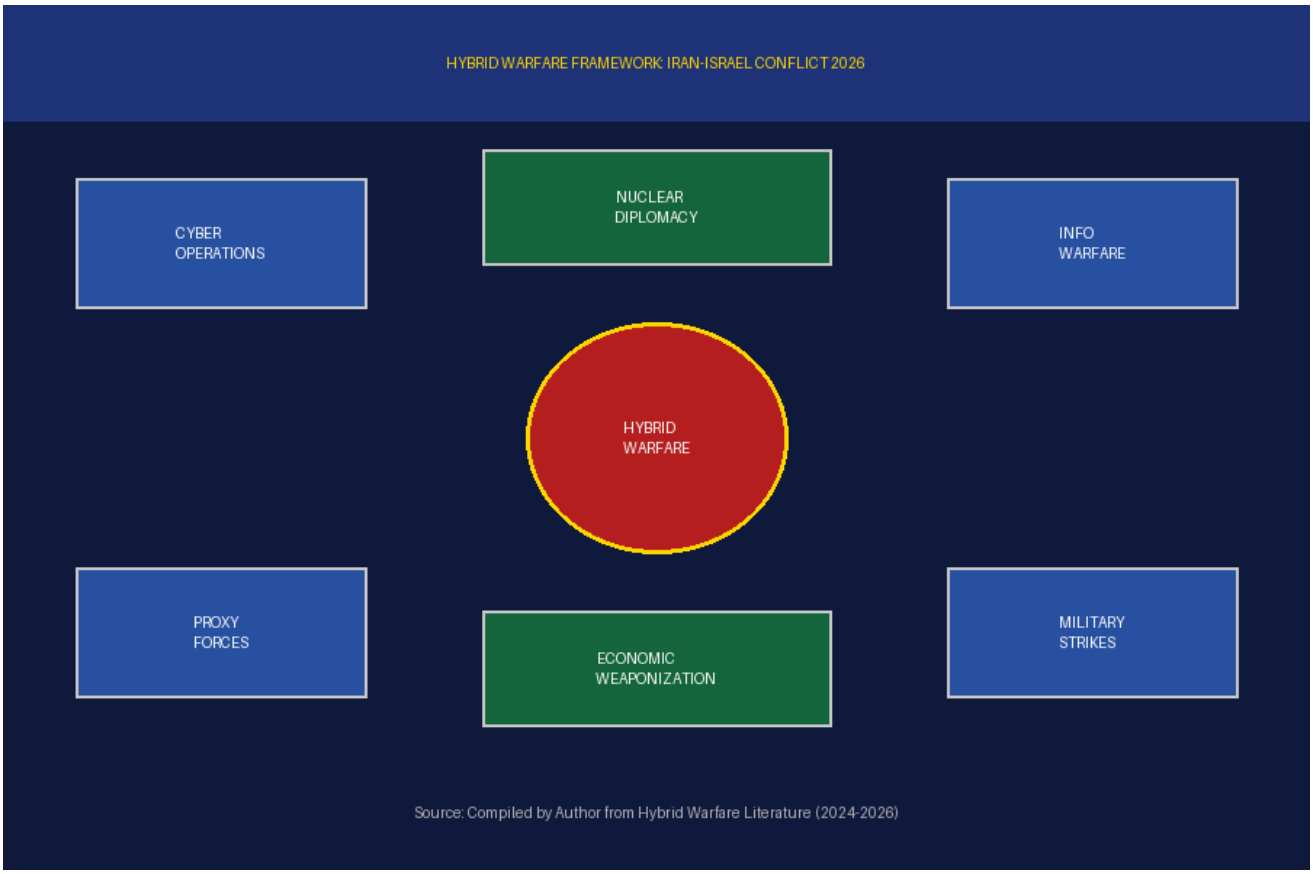


Figure 2: Hybrid Warfare Framework Applied to the Iran–Israel Conflict. Source: Author's Compilation from Hybrid Warfare Literature (2024–2026).

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.04 No.01 (2026)

The rivalry in power on a regional scale literature offers an additional analytical perspective. According to the Regional Security Complex Theory (RSCT) by Buzan and Waever (2003), the security issues in a particular region are highly interdependent as the state and non-state actors are related through the amity-enmity pattern, which determine the conflict relations. An example of a negative security complex is Iran and Israel, both parties in the conflict consider each other a security threat, thus creating a security dilemma that cannot be resolved (Jervis, 1978; Booth and Wheeler, 2008).

The contribution of proxy forces in power contention at the regional level has attracted a lot of academic attention. Salehyan (2010) points out that a state will outsource violence to proxy actors in a bid to realize strategic goals with the plausible deniability and in a way that the risk of a direct retaliation can be limited. The Axis of Resistance of Iran, which includes Hezbollah in Lebanon, Hamas in Gaza, Houthis in Yemen, and other Iraqi militia is the most widespread proxy network in the Middle East (Byman, 2005; Levitt, 2013). The reaction of Israel has involved both kinetic attacks on the infrastructure of proxies and underground attacks against Iranian military and nuclear officials (Bar-Joseph, 2017).

The cyber war is a part of the Iran-Israel conflict that is becoming all the more important in its development. Rid (2013) states that cyber operations are hardly considered acts of war in its traditional sense but are tools of coercive diplomacy and disruption. The Stuxnet attack on the Natanz nuclear facility in Iran (which is commonly believed to have been conducted by Israel and the United States) proved the possibility of cyber operations to have physical impacts and undermine military functions without sparking a traditional war (Zetter, 2014). The further Iranian counterstrikes in terms of cyber activity against Israeli financial and government structures, reported in the Microsoft Digital Defense Report (2024), indicate the process of institutionalization of cyber warfare as a component of hybrid competition.

Another aspect of the hybrid warfare literature is information warfare and psychological operations. Arquilla, and Ronfeldt, (1997) came up with the term netwar to explain conflict that is executed over networked information systems with the focus on the importance of narratives, perceptions and communications infrastructure in influencing the outcomes of conflict. Both Iran and Israel have engaged in extensive information operations in the Iran-Israel case: Iran by using state media, fake accounts on social media, and disinformation campaigns aimed at influencing the opinion of the Israeli populace; and Israel by using strategic communications to legitimize military actions by portraying them as defensive and proportional (Rid, 2020; Betz, 2015).

The development of unmanned aerial vehicles (UAVs) has essentially changed the nature of Iran Iran-Israel war. According to Franke (2021), drone warfare decreases the cost of offensive action, as it lowers its political and human costs. The drone technology that Iran has invested in, such as the use of solar-powered surveillance drones, armed strike drones and swarm systems that can saturate air defenses is a calculated move to take advantage of asymmetries in the conflict (CESCUBE, 2025). The drone industry in Israel is the second most developed worldwide, and it has also used the UAVs to receive intelligence, carry out targeted murders, and strike targets with precision against the infrastructure linked to the Iranians.

The most problematic aspect of the Iran-Israel hybrid confrontation is nuclear coercion. The article by Vipin Narang (2014) on the application of nuclear postures by South Asia and the Middle East provides the asymmetric escalation tactics used by the weaker nuclear ambitions in order to prevent stronger conventional powers. The quest of nuclear breakout capabilities by Iran, to threshold capability by 2025 as assessed by the IAEA, brought a new element to the regional security

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.04 No.01 (2026)

calculus forcing Israel to pursue ever more pre-emptive military postures (Sagan & Waltz, 2012; Pollack, 2019).

The scholarly literature concerning the Twelve-Day War of June 2025 and the 2026 escalation remains in its infancy, yet early evaluations of the June 2025 Twelve-Day War and the subsequent 2026 escalation point to the fact that it represented a qualitative change in the Iran-Israel conflict - no longer a grey-zone conflict, but the open kinetic combat involving a This change questions the current theoretical constructs and requires the re-conceptualization of hybrid warfare that would allow direct conventional warfare as a result of prolonged hybrid escalation.

3. METHODOLOGY

The research design applied in this paper was qualitative research design, which examined the dynamics of the hybrid warfare and regional power rivalry in the Iran and Israel conflict that may occur in 2026. It was conducted as a case study since it enabled a detailed and context-specific analysis of intricate geopolitical, military, and informational relationships in a real-life context (Yin, 2018). Case study approach is especially suitable to investigate such phenomena that are hard to isolate out of their contextual setting and have interacting variables, as is the case with the episodes of hybrid wars (Gerring, 2007).

3.1 Research Design

The study adhered to the interpretivist paradigm, which deals with the comprehension of the formation of hybrid warfare strategies, their application, and perception among the state and non-state actors (Creswell, 2014). The qualitative case study design allowed the researcher to examine various aspects of the conflict such as cyber activities, proxy war, information campaigns and conventional military activities. The interpretivist approach was selected due to its focus on contextual insights and understanding of the importance of subjective meaning-making in geopolitical analysis, which is especially justified in the context of the IranIran Israel conflict as it is a highly contentious and politicized issue.

3.2 Data Collection

Secondary sources have been used to gather data in order to have a multi-perspective and a comprehensive analysis. These sources were: peer-reviewed journal articles on hybrid warfare and Middle Eastern geopolitics; policy documents and reports of international organizations and think tanks like the Council on Foreign Relations, the RAND Corporation, the Begin-Sadat Center; news articles on the subject by reputable international and regional media outlets such as the BBC, Reuters, Al Jazeera and Haaretz; and official documents, press releases, and strategic communication of The sources were chosen according to their trustworthiness, topicality, and timeliness, with the emphasis on the materials published throughout the conflict and the right after it.

3.3 Sampling Strategy

The selection of data sources, which directly touched on the main issues of the Iran-Israel conflict and hybrid warfare approaches, was done through a purposive sampling technique (Patton, 2015). The sources were not excluded based on any geographical aspect and included as long as they contained information about military tactics, cyber operations, information warfare, or the power play within the region. The sources that were redundant or non-analytical were excluded so as to retain analytical depth. The strategy made sure that the dataset was saturated theoretically concerning the research questions of the study.

3.4 Data Analysis

Data collected were analyzed using thematic analysis based on the six phases of Braun and Clarke (2006). This was done through the following steps: familiarizing data by repeatedly reading some of the texts; preliminary coding, which involved identifying recurring patterns and elements of strategy; developing themes, which centered on categories like cyber warfare, proxy engagement, psychological operations, and

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.04 No.01 (2026)

technological integration; and discussing the themes as applied to theories of hybrid warfare and regional power competition. This method was able to identify patterns of underlying trends and strategic actions that shaped the conflict.

3.5 Ethical Considerations

No human subjects were involved in the study since secondary data was used and the available data was in the form of publicly available data. Through proper citation and not misrepresenting data, proper academic integrity was upheld. All citations were done correctly and in compliance with the APA citation guidelines. The researcher was continually conscious of the possibilities of bias on media and policy sources and used the triangulation of different types of sources to reduce interpretive distortions.

4. ANALYSIS AND FINDINGS

The thematic analysis of the existing data revealed that there are five key themes: (1) cyber warfare and digital coercion; (2) mobilization of the proxy force and the Axis of Resistance; (3) information warfare and psychological operations; (4) conventional military escalation and its hybrid antecedents; and (5) nuclear coercive signaling and deterrence dynamics. The analysis of each of the themes is given below.

4.1. Digital Coercion and Cyber Warfare

The cyber activities formed a consistent and more and more centralized aspect of the Iran-Israel hybrid conflict over the years 2023-2026. According to the Microsoft Digital Defense Report (2024), the number of Iranian cyber activities against Israeli organizations grew exponentially: whereas in July-October 2023, 10% of Iranian cyber-attacks were aimed at Israeli organizations, in October 2023, almost half of the attacks were targeted at Israeli organizations (CESCUBE, 2025).

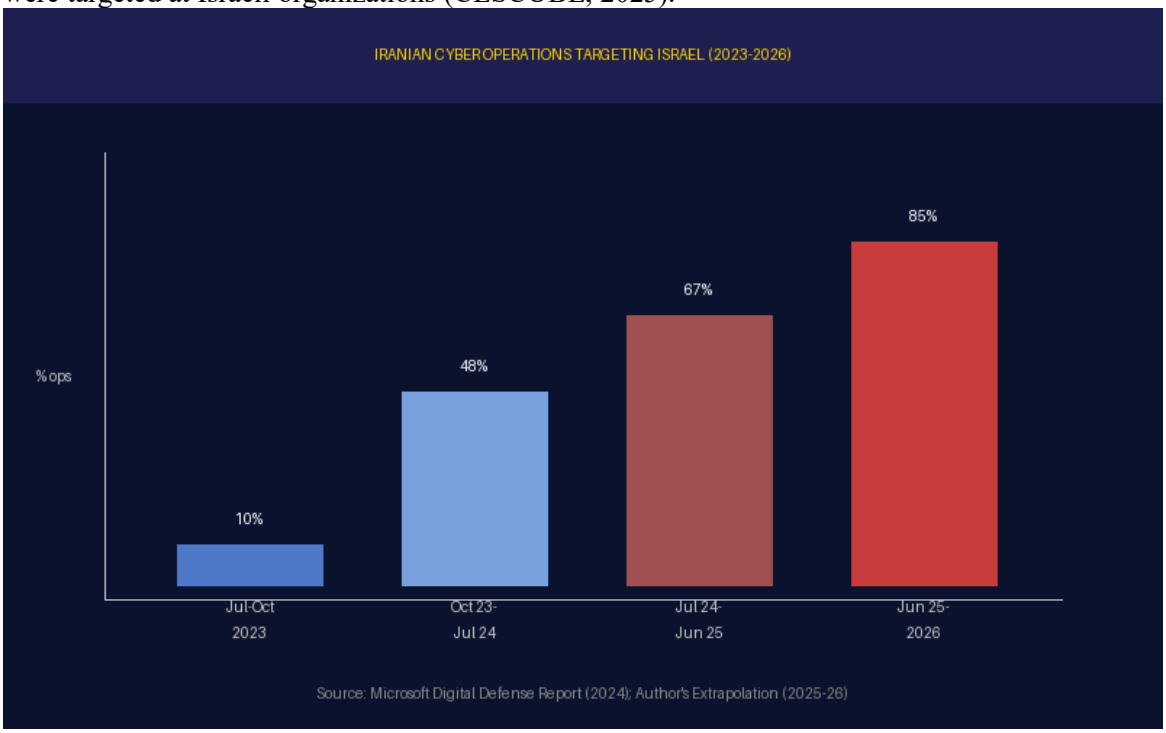


Figure 3: Iranian Cyber Operations Targeting Israel (2023–2026). Source: Microsoft Digital Defense Report (2024); Author's Extrapolation (2025–26).

Iranian cyber-attacks on Israel went into various modalities. Distributed Denial-of-Service (DDoS) attacks were made against Israeli government sites, and financial infrastructure that disrupted the services of the population and eroded trust towards state institutions. Refined phishing attacks targeted senior Israeli government officials, defense officials, academics and journalists and the Israel Shin Bet and National Cyber Directorate reported the blocking of hundreds of these attacks in February 2026 alone (Wikipedia, Iran Iran Israel proxy war, 2026). Iranian fake accounts on social media, including the accounts of fictional

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.04 No.01 (2026)

figures like Tears of War and KarMa have been used to spread disinformation about Israeli military operations and political leadership, both domestically among the Israeli people and internationally (CESCUBE, 2025).

The cyber countermeasures of Israel were no less sophisticated. An offensive cyber campaign by a group of Iranian financial and industrial infrastructure by the so-called Predatory Sparrow (Gonjeshke Darande), often credited to Israeli intelligence, occurred in June 2025, coinciding with the kinetic phase of the Twelve-Day War (CESCUBE, 2025). These actions demonstrate the smooth fusion of cyber warfare with traditional military actions - a hallmark of mature hybrid warfare strategy.

Table 1: Comparative Cyber Warfare Capabilities: Iran vs. Israel (2026)

Dimension	Iran	Israel
Primary Tools	DDoS, phishing, disinformation accounts	Offensive malware, precision cyber strikes
Key Operations	Attacks on Israeli finance/gov, social media ops	Stuxnet (2010), Predatory Sparrow (2025)
Targets	Government officials, financial systems, public opinion	Nuclear facilities, military C2, industrial systems
Coordination	IRGC Cyber Unit, MOIS	Unit 8200, National Cyber Directorate

Source: CESCUBE (2025); Microsoft Digital Defense Report (2024); Wikipedia (2026).

4.2 Proxy Force Mobilization and the Axis of Resistance

The structural support of the hybrid warfare approach towards Israel is the strategic placement of the proxy forces throughout the Middle East. The Axis of Resistance, a raggedly-arranged network of Hezbollah in Lebanon, Hamas in Gaza, and Houthi Movement in Yemen, and several Popular Mobilization Forces (PMF) in Iraq and Syria gave Iran geographic depth, strategic flexibility, and plausible deniability in its conflict with Israel (Byman, 2005; CFR, 2026).



ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.04 No.01 (2026)

Figure 4: Iran's Axis of Resistance: Regional Proxy Network. Source: Author's Compilation (2026).

Although Tehran had no direct role in the October 7, 2023 Hamas attacks on Israel, it was facilitated by years of Iranian material and training assistance, and intelligence exchanges (CFR, 2026). The next stage was the continued rocket and missile attacks on Israeli territory by Hezbollah in Lebanon, the drone and missile attacks on Israeli interests and Red Sea shipping lanes by the Houthis, and the use of Iraqi PMF units to attack US and Israeli interests throughout the region. This multi-front operation of proxy forces was a demonstration of the Iranian concept of forward defense - attacking Israel and the United States in many different ways, but not open direct military conflict (Eisenstadt and Knights, 2014).

Nonetheless, during the 20242026 period, Israeli military operations greatly sabotaged the Iranian proxy network. The assassination of Hezbollah Secretary-General, Hassan Nasrallah, and the decapitation of Hamas political leadership alongside the downfall of the Assad regime in Syria significantly undermined the organizational and operational capabilities of the Axis of Resistance (CFR, 2026). This deterioration of the proxy capabilities could be one of the reasons why Iran decided to go to a full-scale kinetic conflict during the Twelve-Day War of June 2025.

4.3.1 Information Warfare and Psychological Operations.

Iran and Israel also engaged in a massive information warfare during the conflict, to reach local people, regional and the world in general. The information operations of Iran aimed to legitimize the deeds of the Israeli military, cause the Muslim people to stand together and prevent the possibility of the potential allies of the region to fall on the side of Israel or the United States. Media that was state-controlled, such as Press TV and IRNA, conducted the amplification of the discourse of Israeli hostility and Palestinian victimhood, and secret infiltration of social media activities tried to create organic-looking grassroots activism against Israeli policies in Western nations (CESCUBE, 2025).

The information warfare policy of Israel stressed legitimacy of Israeli military actions as self-defense measures against an existential threat. The Israel diplomatic missions and the IDF Spokesperson Unit led the synchronized communication campaigns to present the Twelve-Day War as a pre-emptive strike against a nuclear threat that was about to occur. Israel called the operation Rising Lion, so named due to its symbolic quality, in that it both tapped into the symbolism of Israeli strength and the pre-revolutionary Iranian national icon of the lion, denoting a continuity with a historic Iran that used to be an Israeli ally (RMC Global, 2025).

The information warfare aspect of the confrontation was a manifestation of the growing centrality of perception management in the contemporary hybrid warfare. The art of crafting narratives in networked information space has gained strategic importance, similar to the capacity to cause kinetic damage as Arquilla and Ronfeldt (1997) foresaw. Both Iran and Israel took note of this fact and pumped significant resources into institutional capabilities of information operations, which are also indicative of the larger trends in modern conflict (Rid, 2020).

4.4 Traditional Military Escalation and Hybrid precursors to it.

The June 2025 Twelve-Day War was the climax of years of hybrid warfare sustained over time, and it showed how the competition in the grey-zone can shift to conventional war under certain conditions. The war broke out on June 13, 2025, as Israel went on the offensive in Operation Rising Lion, a surprise attack on Iranian military and nuclear targets, such as the Natanz enrichment facility, Isfahan missile production facilities and the Fordow underground complex (Britannica, 2026; BESA Center, 2025).

The scale of the Israeli offensive had never been seen before: most of the Russian-supplied S-300 air defense systems used by Iran (which had been greatly degraded in the October 2024 exchanges) were taken down by coordinated air attacks, the leaders of the IRGC, nuclear scientists and political figures were targeted, and the United States Air Force was able to strike three Iranian nuclear facilities on June 22, 20 Iran in response fired over 550 ballistic missiles and over 1,000 suicide drones, hitting centers of Israeli civilian population, military bases, and energy facilities. Simultaneously, the Houthis also fired Yemen missiles and the Iranian proxies in Iraq fired at US military installations.

Table 2: Key Military Operations – Twelve-Day War (June 2025) and 2026 Conflict

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.04 No.01 (2026)

Operation	Actor	Targets	Outcome
Rising Lion (Jun 13, 2025)	Israel	Nuclear/military sites, IRGC leaders	Air defenses destroyed; nuclear program set back
Midnight Hammer (Jun 22, 2025)	United States	Fordow, Natanz, Isfahan	Critical nuclear sites heavily damaged
Iranian Missile Barrage	Iran/Houthis	Israeli cities, military bases	550+ ballistic missiles, 1000+ drones; mostly intercepted
Feb 2026 US-Israel Op.	US/Israel	Iranian military, political leadership	Khamenei assassinated; new Supreme Leader appointed
2026 Lebanon War	Israel/Hezbollah	Southern Lebanon, Northern Israel	2,000+ casualties; renewed ground conflict

Source: Wikipedia (Twelve-Day War, 2026); CFR (2026); Britannica (2026); RMC Global (2025).

The war intensified even more in February 2026, when the US and Israeli troops launched a series of attacks on the Iranian military and political elite, causing the assassination of the Supreme Leader Ayatollah Ali Khamenei (Wikipedia, 2026 Iran War; CFR, 2026). It was an unprecedented escalation - a calculated killing of the highest political authority of a sovereign state - with enormous consequences to the international law, the theory of deterrence and the stability of the region. The reaction of Iran involved closing the Strait of Hormuz, missile and drone attacks on US military installations and Gulf Arab nations, and the new Hezbollah activities in Lebanon.

4.5 Nuclear Coercive Signaling and Dynamics of Deterrence.

The Iranian-Israeli nuclear aspect of the conflict is one of the most strategically significant elements of the 2026 conflict. The fact that Iran has reached threshold nuclear capability i.e. the possession of enough enriched uranium to launch nine nuclear warheads as per a June 2025 IAEA report has completely changed the regional deterrence calculus and triggered Israeli pre-emptive military action directly (Wikipedia, Twelve-Day War, 2026; BESA Center, 2025).

The dangers of a pre-emptive attack were less significant than the dangers of an existential threat as seen by Israel with a nuclear armed Iran. The long-held position of Prime Minister Netanyahu that the nuclear program in Iran was a red line to Israeli security was put into action in Operation Rising Lion, when they not only targeted known enrichment facilities but also individuals who were supervising the nuclear program, including those who participated in US-Iran nuclear negotiations (Wikipedia, Twelve-Day War, 2026). The purpose of this targeting of negotiators such as Ali Shamkhani who was leading nuclear negotiations was to both undermine the program and in an indication to the Israeli determination to avert diplomatic protection to further enrichment.

The coercive signaling of Iran in the nuclear front was on several levels. The intentional vagueness of the weaponization timeline, and the continued defiance of the JCPOA and insistence on IAEA inspections following the war in June 2025, served as a deterrence-by-uncertainty to limit the US and Israeli military responses (Narang, 2014; BESA Center, 2025). The international legal and diplomatic context in which the Operation Rising Lion was carried out was the IAEA declaration of non-compliance of Iran one day before the Israeli attack which was proposed by a resolution co-sponsored by the US, UK, France and Germany.

5. DISCUSSION

The empirical data analysis of the 2026 Iran-Israel conflict validates and further elaborates some of the main theoretical theses of the hybrid warfare and regional power rivalry literature. To begin with, the conflict shows that hybrid warfare is not a period or phase of conflict to be transitional or preparatory, but can be a long-term strategic modality that can last decades before progressing to a conventional military conflict. The Iran Israel conflict had gone through different levels, stages and phases, starting with the ideological antagonism and covert operations in the 1980s -1990s, institutionalized proxy competition in

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.04 No.01 (2026)

the 2000s- 2010s, hybrid exchanges direct in 2023-2025 and then pure conventional conflict in 2025-2026. This course of action disputes the fact that much of the literature on hybrid warfare assumes that hybrid strategies are selected as substitutes to conventional conflict as opposed to anticipatory of conventional conflict (Hoffman, 2007; Renz, 2016).

Second, the war depicts how technological asymmetry can be used to develop hybrid warfare dynamics. Investment in drone swarms, ballistic missiles, and cyber operations allowed Iran to confront and not match the Israeli and US conventional military superiority. The multi-layer missile defense system of Israel, including Iron Dome, David's Sling, and Arrow, and the US naval forces in the Eastern Mediterranean showed that integrated air defense against large-scale hybrid attacks with missiles and drones can be effective, with most of the Iranian projectiles being intercepted (Britannica, 2026). Nevertheless, the economic and logistical sustainability issues of interceptor-based defense solutions were demonstrated by the sheer number of the Iranian barrage during the Twelve-Day War alone: more than 550 ballistic missiles and 1,000+ drones (CESCUBE, 2025).

Third, the war shows the changing role of great powers in hybrid warfare in the region. US intervention in the Iran-Israel conflict shifted over time between indirect intervention (sharing of intelligence, shipments of weapons and ammunition) to defensive intervention (interception of missiles) to offensive intervention (Operation Midnight Hammer, February 2026 attacks). This path highlights more general US strategic considerations of the spread of nuclear arms, alliances, and stability in the Middle East, and how external power intervention can decisively influence the dynamics of escalation of regional hybrid conflicts (Waltz, 1979; Mearsheimer, 2001).

The results can be applied to the Regional Security Complex Theory as well (Buzan and Waever, 2003). The conflict of 2026 demonstrates how the Iran-Israel dyad is entrenched in a larger regional security complex that involves the Saudi Arabia, Turkey, Iraq, Lebanon, Yemen, and the Gulf states. The hybrid warfare approach of Iran was clearly meant to exploit this complication - mobilizing proxies on various theater so as to strain the Israeli and US military forces. Nevertheless, the deterioration of the Axis of Resistance under Israeli actions in 2024-2026 implies that the usefulness of the hybrid strategies that rely on proxies is conditional on the organizational soundness and material strength of the proxies (Salehyan, 2010).

6. CONCLUSION AND RECOMMENDATIONS

This paper has explored the hybrid warfare aspects of the Iran-Israel conflict in 2026 based on the theory of hybrid warfare and regional rivalry models of power. It has been found that the conflict was a very evolved and consequence form of multi-domain hybrid warfare, which emphasized cyber operations, proxy mobilization, information campaigns, conventional military strikes, and nuclear coercive signaling into a consistent, although not always coordinated, posture. The progressive path that began with the Gaza War in October 2023 leading to the Twelve-Day War and the US-Israeli operations against the leadership of Iran in June 2025 and February 2026, illustrates how the protracted hybrid competition may result in the escalatory dynamics that eventually lead to the conventional military engagements of historic proportions.

The research has provided various suggestions to policy makers and academicians based on these findings. To begin with, the international community actors need to focus on creating multilateral systems of dealing with the escalation of hybrid warfare, especially in the regions with nuclear ambitions and an active set of proxy networks. Second, states facing hybrid threats should ensure the creation of capabilities and doctrines tailored to multi-domain hybrid environments, not as an extension to conventional military planning of cyber, information, and proxy conflict. Third, the international arms control regime should be revised to capture proliferation of drone technology and cyber weapon, which have become the main tools of hybrid warfare but are not regulated by the current treaties to a large extent.

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.04 No.01 (2026)

In theory, the Iran-Israel conflict of 2026 requires the framework of hybrid warfare to be revised in order to better reflect: the escalatory nature of sustained grey-zone competition; how nuclear thresholds can lead to pre-emptive conventional military action; how proxy network degradation and the direct escalation of conflict both interact; and the role of external great-power intervention in regional hybrid conflicts. Further studies must be conducted to compare the cases of hybrid warfare in other locations, such as the Russia-Ukraine situation or the South China Sea in order to evaluate the generalizability of the patterns of analysis observed in the current study.

The basic motives of Iranian nuclear capability and projection of power in the region are not deterred by the military defeats of 2025 2026. Detailed knowledge of the hybrid warfare dynamics considered in this research is thus necessary to policy-makers, military practitioners and academics attempting to operate in an ever-expanding and perilous regional security landscape within the Middle East and beyond (BESA Center, 2025).

REFERENCES

Arquilla, J., & Ronfeldt, D. (1997). In Athena's camp: Preparing for conflict in the information age. RAND Corporation.

Bar-Joseph, U. (2017). The angel: The Egyptian spy who saved Israel. HarperCollins.

Begin-Sadat Center for Strategic Studies [BESA]. (2025). The Israel-Iran War: Israel's new strategic opening. BESA Center Publications.

Berzins, J. (2014). Russia's new generation warfare in Ukraine: Implications for Latvian defense policy (Policy Paper No. 02). National Defence Academy of Latvia.

Betz, D. (2015). Carnage and connectivity: Landmarks in the decline of conventional military power. Oxford University Press.

Blanford, N. (2011). Warriors of God: Inside Hezbollah's thirty-year struggle against Israel. Random House.

Booth, K., & Wheeler, N. J. (2008). The security dilemma: Fear, cooperation and trust in world politics. Palgrave Macmillan.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77-101. https://doi.org/10.1191/1478088706qp063oa

Britannica. (2026). 12-Day War. Encyclopaedia Britannica. https://www.britannica.com/event/12-Day-War

Buzan, B., & Waever, O. (2003). Regions and powers: The structure of international security. Cambridge University Press.

Byman, D. (2005). Deadly connections: States that sponsor terrorism. Cambridge University Press.

Center for Strategic and Cubic Excellence [CESCUBE]. (2025). Iran-Israel conflict and the future of asymmetric warfare in the Middle East. CESCUBE Publications.

Chubin, S. (2009). Iran's nuclear ambitions. Carnegie Endowment for International Peace.

Council on Foreign Relations [CFR]. (2026). Global conflict tracker: Confrontation between the United States and Iran. https://www.cfr.org

Creswell, J. W. (2014). Research design: Qualitative, quantitative, and mixed methods approaches (4th ed.). SAGE Publications.

Eisenstadt, M., & Knights, M. (2014). Beyond symmetry: The "1,000 cuts" approach to countering Iran's use of proxies in the Middle East. PolicyWatch, The Washington Institute for Near East Policy.

Franke, U. (2021). Drones in conflict zones: The new normal? European Union Institute for Security Studies.

Galeotti, M. (2016). Hybrid, ambiguous, and non-linear? How new is Russia's "new way of war"? Small Wars & Insurgencies, 27(2), 282-301. https://doi.org/10.1080/09592318.2015.1129170

Gerring, J. (2007). Case study research: Principles and practices. Cambridge University Press.

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.04 No.01 (2026)

Hoffman, F. G. (2007). Conflict in the 21st century: The rise of hybrid wars. Potomac Institute for Policy Studies.
Hoffman, F. G. (2009). Hybrid threats: Reconceptualizing the evolving character of modern conflict. Institute for National Strategic Studies Strategic Forum, (240), 1-8.
Jervis, R. (1978). Cooperation under the security dilemma. World Politics, 30(2), 167-214. https://doi.org/10.2307/2009958
Johnson, R. (2018). Hybrid war and its countermeasures: A critique of the literature. Small Wars & Insurgencies, 29(1), 141-163.
Kofman, M., & Rojansky, M. (2015). A closer look at Russia's "hybrid war." Kennan Cable, (7). Wilson Center.
Levitt, M. (2013). Hezbollah: The global footprint of Lebanon's party of God. Georgetown University Press.
Lind, W. S., Nightengale, K., Schmitt, J. F., Sutton, J. W., & Wilson, G. I. (1989). The changing face of war: Into the fourth generation. Marine Corps Gazette, 73(10), 22-26.
Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. Security Studies, 22(3), 365-404.
Mazarr, M. J. (2015). Mastering the gray zone: Understanding a changing era of conflict. US Army War College Press.
McCulloh, T., & Johnson, R. (2013). Hybrid warfare. JSOU Report, 13(4). Joint Special Operations University.
Mearsheimer, J. J. (2001). The tragedy of great power politics. W.W. Norton.
Microsoft. (2024). Microsoft Digital Defense Report 2024. Microsoft Corporation.
Murray, W., & Mansoor, P. R. (Eds.). (2012). Hybrid warfare: Fighting complex opponents from the ancient world to the present. Cambridge University Press.
Narang, V. (2014). Nuclear strategy in the modern era: Regional powers and international conflict. Princeton University Press.
Patton, M. Q. (2015). Qualitative research and evaluation methods (4th ed.). SAGE Publications.
Pollack, K. (2019). Unthinkable: Iran, the bomb, and American strategy. Simon & Schuster.
Renz, B. (2016). Russia and "hybrid warfare." Contemporary Politics, 22(3), 283-300.
Rid, T. (2013). Cyber war will not take place. Oxford University Press.
Rid, T. (2020). Active measures: The secret history of disinformation and political warfare. Farrar, Straus and Giroux.
RMC Global. (2025). Israel-Iran conflict: 2025 update. RMC Global Intelligence. https://rmcglobal.com
Sagan, S. D., & Waltz, K. N. (2012). The spread of nuclear weapons: An enduring debate (3rd ed.). W.W. Norton.
Salehyan, I. (2010). The delegation of war to rebel organizations. Journal of Conflict Resolution, 54(3), 493-515.
Takeyh, R. (2021). The last shah: America, Iran, and the fall of the Pahlavi dynasty. Yale University Press.
Waltz, K. N. (1979). Theory of international politics. Addison-Wesley.
Wikipedia. (2026a). 2024 Iran-Israel conflict. Wikimedia Foundation.
Wikipedia. (2026b). Iran-Israel proxy conflict. Wikimedia Foundation.
Wikipedia. (2026c). Twelve-Day War. Wikimedia Foundation.
Wikipedia. (2026d). 2026 Iran war. Wikimedia Foundation.
Yin, R. K. (2018). Case study research and applications: Design and methods (6th ed.). SAGE Publications.
Zetter, K. (2014). Countdown to zero day: Stuxnet and the launch of the world's first digital weapon. Crown Publishers.